MYKOLO ROMERIO UNIVERSITETO
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETO
INFORMATIKOS IR STATISTIKOS KATEDRA

SIGITA LAPINSKAITĖ
DIENINIO SKYRIAUS INFORMATIKOS TEISĖS PROGRAMA

SPAM TEISINIS REGULIAVIMAS - LYGINAMASIS ASPEKTAS

Magistro baigiamasis darbas

Darbo vadovas –
doc. dr. Darius Štitilis

Vilnius, 2008

TURINYS

ĮVADAS

Naudojimasis informacinėmis technologijomis daugeliui žmonių tampa kasdieninio gyvenimo dalimi. Vis dažniau komunikuojama elektroninėje erdvėje, ypač išpopuliarėjo elektroninis paštas. Tačiau elektroniniu paštu keliauja ne vien svarbi ir respondentų laukiama informacija, bet ir nelaukiami, daugiausiai komercinio pobūdžio elektroniniai laiškai, kurie vadinami *spam*.

Spam paprastai suprantamas kaip nepageidaujamų elektroninių laiškų siuntimas dideliais kiekiais asmenims, kurie jų nepageidavo, dažniausiai komerciniais, tiesioginės rinkodaros tikslais. Lietuvių kalbos inspekcija siūlo terminui *spam* naudoti sąvoką „interneto šiukšlės“ arba „brukalas“, tačiau tiek mokslinėje literatūroje, tiek šnekamojoje kalboje dažniau yra naudojamas *spam* terminas.

Nepaisant teisės aktais nustatytų draudimų, daugėja asmenų (*spamerių)*, kurie per dieną išsiunčia milijonus elektroninių pranešimų, siūlančių viską – nuo pigių paskolų iki pornografijos, dėl to *spam* skaičiumi aplenkė net teisėtus elektroninio pašto laiškus. Šiuo metu net 73,3 proc. viso pasaulio elektroninio pašto srauto sudaro *spam* (2001 m. *spam* paplitimas buvo 7 proc.)[1], taip pat ir Lietuvoje, *spam* pranešimų išsiunčiama vis daugiau. *Spam* tampa problema tiek informacinių technologijų vartotojams, tiek informacinių technologijų paslaugų tiekėjams; dėl *spam* srautų apkraunami elektroninių ryšių tinklai, įvairios pasaulio kompanijos patiria milijardus nuostolių, mažėja darbuotojų produktyvumas, pažeidžiami asmens privatumo, orumo bei laisvo apsisprendimo principai, įtvirtinti valstybių konstitucijose, tarptautinėse konvencijose.

Nepageidaujami elektroniniai pranešimai dabar vis dažniau yra apgaulingo ir nusikalstamo pobūdžio, pavyzdžiui, duomenis vagiantys elektroninio pašto pranešimai (angl. *phishing*), kurie iš vartotojų per tikrų įmonių interneto svetainių imitacijas išvilioja konfidencialius duomenis, taip pat elektroniniu paštu plintančios įvairios šnipinėjimo programos, kuriomis sekami vartotojo veiksmai internete bei renkama asmeninė informacija, pavyzdžiui, slaptažodžiai ar kredito kortelių numeriai. Tokiais neteisėtais būdais be asmens sutikimo surinkus asmens duomenis bei panaudojus juos prekių, paslaugų įsigijimui to asmens vardu, kyla tapatybės vagystės pavojus. Masinį nepageidaujamo elektroninio pašto pranešimų siuntimą palengvina žalingų kodų, pavyzdžiui, „kirminų“, „Trojos arklių“ ir kitų virusų platinimas, kuriuos įdiegus, užpuolikas gali perimti užkrėstos kompiuterių sistemos valdymą ir ją paversti „zombiu“[2] (angl. *botnet*), paslėpdamas tikrojo nepageidaujamo elektroninio pašto platintojo

[1] Apie spam faktais // http://www.esaugumas.lt/index.php?1812607726; prisijungimo laikas: 2008-12-02.

[2] *Zombiai* (angl. *zombie*) –tai užkrėsti kompiuteriai, kuriuos *spam* platintojai naudoja dideliems elektroninių pranešimų kiekiams siųsti, įdiegę paslėptą programinę įrangą, kuri kompiuterius, vartotojams nežinant, paverčia pašto serveriais.

tapatybę. Tokių šnipinėjimo programų ir kitų žalingų virusų, puolančių vartotojų ir įmonių kompiuterius, plitimas daro didelį poveikį ekonomikai bei didina vartotojų nepasitikėjimą elektroninio pašto paslauga, kartu kenkia ir įmonių reputacijai.

Dėl *spam* keliamų grėsmių dydžio ir masto, su *spam* plitimu kovoja privataus sektoriaus kompanijos, naudodamos technines priemones bei diegdamos *anti-spam* programas, tačiau vien šių techninių priemonių neužtenka. Siekiant sustabdyti *spam* plitimą, jį reguliuoti ir nustatyti atsakomybę *spameriams*, turi būti kuriama teisinė bazė. Atskiros valstybės, taip pat įvairios tarptautinės grupės ir organizacijos, tokios kaip Europos ekonominio bendradarbiavimo ir plėtros organizacija (EBPO) (programa „Anti - Spam Toolkit“), Tarptautinė telekomunikacijų sąjunga (angl. *International Telecommunications Union - ITU*) taip pat įsijungė į šią kovą. Organizuojami įvairūs tarptautiniai susivienijimai ir kuriami specialūs *anti-spam* projektai (pvz., „*Spam Zombie“, „London action plan*“), į jų veiklą įtraukiami ir interneto paslaugų teikėjai (toliau - IPT). JAV Federalinė prekybos komisija (*angl. trump. FTC*) šiuo metu ypač aktyviai bendradarbiauja su Europos Sąjungos institucijomis, teikia rekomendacijas ir pasiūlymus tarptautiniu mastu. Diegiamos įvairios *anti-spam* kompiuterinės programos, naudojamos naujos technologijos.

Spam teisinis reguliavimas ir atskirų valstybių priimtų teisės normų tyrimas tampa vis aktualesnis tiek dėl vis didėjančios *spam* problemos kasdieniniame gyvenime, tiek dėl šio reiškinio globalumo sukeliamų implikacijų: elektroninė erdvė plisti naujiems su *spam* siuntimu susijusiems teisės pažeidimams yra atvira visoms valstybėms, o neegzistuojant geografinėms sienoms, iškyla atskirų valstybių skirtingo *spam* reglamentavimo, teisinės jurisdikcijos bei atsakomybės nustatymo problemos. Pavyzdžiui, yra manoma, kad spam problemos iškėlimą ir atitinkamai sprendimų ieškojimą apsunkina pasaulyje vieningos *spam* definicijos nebuvimas. Be to, vienose valstybėse *spam* traktuojamas kaip nusikaltimas ir taikoma baudžiamoji atsakomybė, kitose – kaip civilinės ar administracinės teisės pažeidimas. Todėl yra aktualu nagrinėti ir lyginti įvairiose šalyse už *spam* plitimą atsakingų valstybės institucijų priimtų teisės aktų normas, jų ypatumus bei veiksmingumą, siekiant apginti elektroninio pašto savininko ir interneto paslaugų teikėjų teises.

Į kovą prieš *spam* įsitraukusios naujos valstybės ir organizacijos priima naujus, ir papildo iki tol galiojusius teisės aktus, dėl to ši teisės sritis yra dinamiška ir greitai besivystanti, tad svarbu, kad ankstesnių autorių atliktą analizę bei tyrimus *spam* teisinio reguliavimo tema papildytų nauji moksliniai darbai apie naujausias tendencijas *spam* reglamentavimo srityje.

Lyginamuoju aspektu *spam* teisinio reguliavimo tema Lietuvoje dar nebuvo analizuota. S. Toliušis bei Mykolo Romerio universiteto doc. dr. D. Štitilis knygoje „Informacinių technologijų teisė“ (2004 m.) yra nagrinėję apsisprendimo teisės internete bei asmens duomenų

apsaugos internete aspektus, kurie iš dalies apima ir *spam* problematiką. Taip pat doc. dr. D. Štitilis yra analizavęs kompiuterinius nusikaltimus, jų kriminalizavimą Lietuvoje, teisės į privatumą pažeidimus bei kompiuterinių pažeidimų teisinį reglamentavimą vadovėlyje „Informatikos teisė ir teisės informatika“ (2006 m.). Nors *spam* taip pat gali būti laikomas vienu iš kompiuterinių nusikaltimų (pvz., JAV), tačiau *spam* problemos analizė lyginamuoju aspektu nebuvo atlikta.

Darbo tikslas. Pagrindinis šio mokslinio tiriamojo darbo tikslas – lyginamuoju aspektu išnagrinėti *spam* teisinį reglamentavimą ir su juo susijusias teisines problemas.

Siekiant kuo didesnio reprezentatyvumo viso pasaulio mastu, analizei be Lietuvos (kurios teisinis reglamentavimas atspindi Europos Sąjungos poziciją *spam* atžvilgiu) buvo pasirinktos dar 4 pasaulio valstybės iš skirtingų kontinentų: JAV, Rusija, Australija ir Argentina. Šios valstybės aktyviai diegia informacines technologijas ir yra priėmusios su *spam* reglamentavimu susijusius teisės aktus, kurie yra viešai pateikiami/prieinami anglų kalba.

Darbo uždaviniai:

1) Atskleisti *spam* sampratą ir jo ypatumus.

2) Išanalizuoti pagrindinius teisės aktus, reglamentuojančius *spam* Lietuvoje, JAV, Rusijoje, Australijoje ir Argentinoje bei atskleisti su *spam* reglamentavimu susijusias teisines problemas pagal pasirinktus kriterijus.

3) Atliekant empirinį tyrimą, išanalizuoti, kaip įgyvendinami elektroniniam komerciniam pranešimui keliami reikalavimai bei užtikrinamas *spam* atsisakymas ir kokia yra teisės įtaką *spam* reiškiniui.

4) Pateikti galimus teisinius *spam* problemos sprendimo būdus, teisines situacijos gerinimo galimybes.

Darbo objektas - *spam* teisinis reglamentavimas.

Darbo metodai: lyginamasis metodas ir dokumentų analizės metodas.

Darbo šaltiniai: Australijos, Argentinos, Rusijos, JAV ir Lietuvos Respublikos teisės aktai, Tarptautinių organizacijų (ITU, OECD) bei ES norminiai teisės aktai, straipsniai Internete, Lietuvos ir užsienio mokslinė literatūra bei teismų praktika.

1. *SPAM* SAMPRATA IR JO YPATUMAI

Viena iš pagrindinių žmogaus teisių yra įsitikinimų, idėjų ir kalbos laisvė. Jungtinių Tautų Visuotinėje Žmogaus teisių deklaracijoje teigiama, kad „Kiekvienas žmogus turi teisę į įsitikinimus ir jų reiškimo laisvę, kuri apima teisę nekliudomai laikytis savo įsitikinimų ir teisę ieškoti, gauti ir skleisti informaciją ir idėjas nepriklausomai nuo valstybių sienų, iš nesvarbu, kokiomis priemonėmis jos būtų išreikštos“[3]. Šios nuostatos įvairiu lygmeniu yra perkeltos į daugelio demokratinių valstybių konstitucijas. Vis dėlto išraiškos laisvė, laisvas kalbėjimas, informacijos kūrimas ir skleidimas nėra absoliučios teisės ir gali būti varžomos siekiant apsaugoti asmens privatumą, konfidencialumą, viešą saugumą, valstybės paslaptis. Šioje deklaracijoje minima išraiškos laisvė nesuteikia teisės įžeisti asmenį, jam primygtinai siūlyti savo idėjas bei pažiūras ir likti nenubaustam. Deklaracija nenustato ir tam tikros asmens prievolės priimti korespondenciją (konkrečiai elektroninio pašto laiškus). Tačiau analizuojant šiandienines aktualijas pastebima, kad ne visada laikomasi Deklaracijos nuostatų.

Atsiradusios naujos IKT sudaro palankias galimybes piktnaudžiauti kalbos laisve, t.y. siųsti nepageidaujamus elektroninius komercinius pranešimus, kitaip vadinamus elektroninėmis šiukšlėmis, arba ***spam***. Šis reiškinys egzistavo ir anksčiau, tačiau atsiradęs Internetas tapo itin parankia priemone jam plisti.

Šiam darbui pasirinkta sąvoka ***spam***. Analizuojant šį terminą, pastebėtina, kad žodis ***spam*** nėra bendrinės anglų kalbos žodis, kuriam priskirta papildoma „internetinė“ reikšmė. Tai tik sukurtas pavadinimas – kelių žodžių junginių trumpinys (SPAM - S (*ending*) P (*eople*) A(*nnoying*) M (*essages*)[4] – liet. erzinančių pranešimų siuntimas asmenims), kuris dėl plataus šio reiškinio paplitimo tampa bendrinės kalbos žodžiu. Šiuo žodžiu nusakomas ne tik nepageidaujamas, erzinantis pranešimas, bet ir visas tokių pranešimų platinimo reiškinys. Šis terminas prigijo ir lietuvių kalboje. Anglų kalba ***spam*** gali būti vadinamas ir kitais pavadinimais: „šlamštu“ (angl. „*junk mail*“), „masiniu laišku“ (angl. „*bulk mail*“), „neprašytu komerciniu laišku“ (angl. „*uncolicited commercial email*“).

Analizuojant ***spam*** fenomeną, nėra priimta vieninga ir konkreti definicija jam apibrėžti, nes yra skirtingų šio reiškinio interpretacijų bei daugybė ***spam*** turinio ir išraiškos formų. „2005 m. kovo mėnesio specialiosios paskirties grupės spam (elektroninio pašto šiukšlių) klausimui nagrinėti (angl. „Spam Task Force“) parengtame EBPO dokumente „Kovos su spam nuostatos“ (angl. „Anti Spam Regulations“) (DSTI/CP/ICCP/SPAM(2005) 1 apibūdinant spam sampratą

[3] 1948 m. Jungtinių Tautų Visuotinė Žmogaus teisių deklaracija // Valstybės žinios, 2006-06-17, Nr. 68-2497
[4] I. Jarukaitis, T. Lamanauskas, M. Civilka ir kiti. Elektroninių ryšių teisė. - Vilnius: Eugrimas, 2005.P.352

teigiama: „Terminas spam paprastai naudojamas tarptautinėje žiniasklaidoje ir įvairių šalių politikos pranešimuose, tačiau nėra bendrai naudojamo šio termino apibrėžimo. Nors kalbama apie tą patį reiškinį, skirtingos šalys apibrėžia spam tuo būdu, kuris yra tinkamiausias vietos aplinkai. Vystant kovos su spam politiką, būtina aiškiai suprasti ir apibrėžti spam prigimtį, atskiriant spam siuntimą nuo teisėtos veiklos.“[5] Reikėtų paminėti, kad šiame moksliniame tiriamajame lyginamajame darbe vieningas *spam* terminas bus naudingas dar ir dėl to, kad būtų galima vienu vardu vadinti ir analizuoti skirtingai valstybių teisės aktuose apibrėžiamą *spam* terminą.

Vertėtų pirmiausiai apžvelgti *spam* bruožus, kurie geriausiai apibūna šį reiškinį: visų pirma, *spam* yra elektroninis pranešimas. Dėl daugybės tikslų spam priskiriamas elektroniniam paštui, bet egzistuoja ir kitos *spam* platinimo galimybės ir formos. “Nauja tendencija ta, kad šiukšlės „persikelia“ ir į judriuosius tinklus. Pavyzdžiui, 2003 m. Japonijoje 90 procentų šiukšlių buvo siunčiama į judriojo ryšio telefonus“ [6]. Vadinasi, *spam* gali būti platinamas pranešimų gaviklių bei mobiliojo telefono pagalba, siunčiant trumpąsias žinutes (SMS), balso pašto ir kitus pranešimus.

Antra, *spam* yra nepageidaujamas, neprašytas (angl. *unsolicited*), t.y. be vartotojo sutikimo siunčiamas laiškas. Jei gavėjas yra išreiškęs pritarimą, t.y. pageidauja, gauti pranešimą, tai tuomet šis pranešimas nebus laikomas *spam* ir bus laikomas teisėtai gautu elektroniniu komerciniu pranešimu. Todėl šalia nepageidaujamumo požymio būtų galima įvardinti, neteisėtumo, t.y. prieštaravimo teisei, požymį, nes kaip pastebėsime nagrinėdami atitinkamų valstybių teisės aktus, sutikimas (pageidavimas) yra viena pagrindinių sąlygų teisėtam elektroniniam komerciniam pranešimui. Vis dėlto nėra aišku, kaip ir kada iki atsirandant santykiui tarp siuntėjo ir gavėjo šitas sutikimas turėtų būti duotas ar išreikštas. Daug priklauso nuo valstybių pasirinkimo taikyti sutikimo (angl. *opt –in*) ir atsisakymo (angl. *opt – out*) metodus, kurie išsamiau aptarti 2.2.1. skirsnyje.

Trečia, *spam* siunčiamas masiškai (angl. *in bulk*). Tai reiškia, kad siuntėjas platina didelį skaičių vienodų, tapačių pranešimų ir kad šie pranešimai yra išsiunčiami nurodant bet kokių pasirinktų gavėjų adresus. Elektroniniai laiškai išsiunčiami keliems šimtams ar tūkstančiams adresatų naudojant kompiuterį, elektroninių ryšių tinklus, elektroninį paštą, judriojo ryšio (telefonais siunčiama SMS) ar kitus elektroninės komunikacijos būdus ir priemones. Kai kuriose valstybėse, pvz., JAV, yra apibrėžta, kas yra masinis pranešimų siuntimas: jei išsiunčiama daugiau nei 100 elektroninio pašto pranešimų per 24 valandų

[5] 29 straipsnio darbo grupės nuomonė 2/2006 apie privatumo klausimus susijusius su elektroninio pašto tikrinimo paslaugų teikimu // http://www.oecd.org/dataoecd/5/47/34935342.pdf; prisijungimo laikas 2008-06-02.
[6] I. Jarukaitis, T. Lamanauskas, M. Civilka ir kiti. Elektroninių ryšių teisė. – Vilnius: Eugrimas, 2005. P. 353.

laikotarpį, jei išsiunčiama daugiau nei 1000 elektroninio pašto pranešimų per 30 dienų laikotarpį arba jei išsiunčiama 10 000 elektroninio pašto pranešimų per vienerių metų laikotarpį.

Ketvirta, *spam* gali būti komercinio pobūdžio ir platinamas siekiant parduoti įvairias prekes, reklamuoti paslaugas internete. Komercinis pranešimas gali būti suvokiamas kaip „bet kokia pranešimo forma, skirta tiesiogiai arba netiesiogiai reklamuoti prekes, paslaugas ar įmonės, organizacijos ar asmens, besiverčiančio komercine, pramonine ar amatų veikla arba reglamentuojama profesija, vardą“[7]. Tam tikros įmonės, dažniausiai mažos, taupydamos pinigus, reklamuoja ir parduoda savo prekes ar paslaugas naudodamos pigią priemonę - elektroninį laišką, kaip „komercinį pranešimą“. Kartais jos užsako *spamerius* ir jiems sumoka atlygį už šią nelegalią paslaugą. *Spameriai* per akimirką išsiunčia pranešimus tūkstančiams asmenų, su kuriais reklamuojamų prekių savininkas anksčiau nepalaikė jokių ryšių. Toks reklamos platinimas yra griežtai draudžiamas ir apibrėžtas daugelio pasaulio šalių įstatymuose. Beje, įdomus faktas tas, kad „2006 m. tinklų ir informacijos saugumo būklės tyrimo (toliau-tyrimo) duomenimis, 96 proc. interneto paslaugų vartotojų niekada nėra įsigiję tokiu būdu siūlomų prekių ar paslaugų. Tik 1 proc. tiesioginės apklausos dalyvių nurodė, kad dažnai įsigyja prekių ar paslaugų, siūlomų nepageidaujamais komerciniais pranešimais“[8]. Vadinasi, komercinio/reklaminio pobūdžio *spam* yra ne tik teisiškai draudžiamas, bet ir iš dalies įmonėms finansiškai nenaudingas bei atneša nemažai žalos elektroninio pašto savininkui.

Penkta, *spam* gali būti kenkėjiško pobūdžio, t.y. su *spam* keliaujantys kompiuteriniai virusai, taip vadinami interneto „kirminai“ ir *Trojos* virusai. Dažnai tai būna kompiuterinės programos, skenuojančios virusu infekuoto kompiuterio atmintį, ieškant elektroninio pašto adresų, kuriais būtų galima persiųsti virusą kitai potencialiai aukai. Taip pat sparčiai plinta laiškai-žvejai (*angl. phishing*), kurie siunčiami sukčių siekiant išgauti iš aukos vertingą informaciją. Prieš kelerius metus Jungtinėse Amerikos Valstijose (toliau – JAV) FTB netgi buvo sukurtas naujas skyrius kovai su *spam*, nes vis labiau įsigalintis *spam* ne tik „užkemša“ elektroninio pašto dėžutes, tačiau jo pagalba vykdomi elektroninio – finansinio pobūdžio nusikaltimai.

Taigi remiantis šiais išvardintais požymiais, būtų galima išskirti du *spam* suvokimo aspektus: 1) (siaurąja prasme) tai nepageidaujamas elektroninis komercinis pranešimas, kurį siunčia įmonės rinkodaros, marketingo, komerciniais, reklamos tikslais; 2) (plačiąja prasme) tai masiškai siunčiamas nepageidaujamas elektroninis pranešimas, kurio turinys nebūtinai turi būti komercinio, tačiau yra kenkėjiško arba amoralaus pobūdžio, arba yra skirtas sukčiams gauti

[7] Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1.
[8] Z. Medutis. Nepageidaujamų elektroninio pašto pranešimų studija // http://www.ada.lt/images/cms/File/Inspekcijos %20rekomendacijos/NEPP%20studija1.pdf; prisijungimo laikas: 2008-11-02.

materialinės naudos, arba visiškai beprasmio turinio pranešimas, kuris skirtas apkrauti interneto tinklus.

O apskritai *spam* – „tai nepageidaujama (nesant informacijos gavėjo sutikimo ar prašymo) ir (ar) nepageidautina (prieštaraujant informacijos gavėjui) plataus masto, dažniausiai reklaminiais komerciniais tikslais (visada siekiant gauti tam tikrą naudą) elektroniniu paštu siunčiama įvairi informacija, apkraunanti informacines sistemas bei interneto vartotojų elektroninio pašto dėžutes ir atnešanti žalą fiziniams ir juridiniams asmenims.“ [9]

Eiliniam vartotojui tai tiesiog žinutės, kurių nenorima matyti asmeninėje elektroninio pašto dėžutėje.

[9] M. Kiškis, R. Petrauskas, I. Rotomskis ir kt. Teisės informatika ir informatikos teisė: vadovėlis. - Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006. P. 125.

2. LIETUVOS IR UŽSIENIO VALSTYBIŲ *SPAM* REGLAMENTAVIMO YPATUMAI LYGINAMUOJU ASPEKTU

Suvokiant *spam* kaip problemą ir ieškant sprendimo būdų, itin reikšmingas yra teisinio reguliavimo priemonių kūrimas ir jų taikymas. Tokios valstybės kaip Australija, Belgija, Kinija, Japonija, Lietuva (ES), Nyderlandai ar JAV jau yra priėmusios specialiuosius *spam* reguliuojančius norminius teisės aktus. Kitos valstybės, pavyzdžiui, Argentina, Brazilija, Honkongas, Rusija, Singapūras tokių teisės aktų neturi, tačiau yra tam tikri siūlymai priimti specialiuosius *anti-spam* teisės aktus. Yra tokių valstybių, pavyzdžiui, Bulgarija, Čilė, Malaizija, Meksika, Peru, Šveicarija, kurios neturi specialiųjų *anti-spam* teisės aktų, bet naudoja alternatyvius teisės aktus, tokius kaip vartotojų apsaugos įstatymas, duomenų apsaugos įstatymas ir taiko juos *spam* problemoms spręsti. Tokios valstybės kaip Bangladešas, Burkina Fasas, Salvadoras, Kuveitas, Madagaskaras, Moldova, Libanas apskritai neturi nei specialiųjų, nei alternatyviųjų *spam* reglamentuojančių teisės aktų (priedas Nr. 2). Šis skirtingų lygių *spam* įstatyminės bazės egzistavimas ar apskritai jos nebuvimas parodo, kad *spam* kaip tarptautinę problemą bus sunku spręsti, kadangi nemaža dalis pasaulio valstybių savo teisės aktuose apskritai nėra įvardijusios *spam* reiškinio kaip problemos, o jei ir pripažįsta minėtą problemą, nekuria teisinių priemonių jai įveikti ir sudaro nišą plisti teisės pažeidimams globalioje interneto erdvėje. Šiame skyriuje, siekiant atskleisti vis gilėjančios *spam* problemos priežastis, naudojant lyginamąjį ir dokumentų analizės metodus, bus analizuojami skirtingoms kategorijoms priklausančių 5 valstybių *spam* reglamentuojantys teisės aktai ir jų normos pagal šiuos kriterijus: a)nagrinėjant teisės aktuose įtvirtintas spam definicijas, bus aiškinamasi ar visur *spam* įvardijamas ir suvokiamas kaip tas pats reiškinys; b) kiek plačiai yra reglamentuotas elektroninių komercinių pranešimų siuntimas bei turinys ir kokių prievolių turi laikytis elektroninių komercinių pranešimų siuntėjai; c) kokios atsakomybės ribos yra nustatytos už prievolių nesilaikymą ir elektroninio pašto vartotojų teisių pažeidimą, paliečiant ir jurisdikcijos elektroninėje erdvėje probleminius kausimus.

2.1. *Spam* sąvokos apibrėžtumo skirtumai ir panašumai

Analizuojant 5 pasirinktų valstybių, patenkančių į skirtingas *spam* teisėkūros išsivystymo ir egzistavimo kategorijas, teisės aktus, pastebėta, kad net *spam* sąvoka priimtuose teisės aktuose yra įvardijama skirtingai. *Spam* reiškinys turėtų būti apibrėžiamas vienodai, kad būtų galima aiškiai suvokti, kur yra riba tarp teisėtai siunčiamų elektroninių komercinių pranešimų ir *spam*.

Europos Sąjungos, tuo pačiu ir Lietuvos, teisės aktuose apskritai tokie terminai kaip *spam* ar nepageidaujamas elektroninis komercinis pranešimas nėra nei apibrėžtas, nei vartojamas. 2002 m. Asmens duomenų ir privatumo apsaugos e-ryšių sektoriuje direktyvos 2002/58/EC[10] 13 straipsnyje *spam* įvardijamas kaip „neužsakyti pranešimai“, kurie siunčiami tiesioginės rinkodaros tikslais (angl. *unsolicited communications*), 2000 m. Elektroninės komercijos direktyvos 2000/31/EC[11], 7 straipsnyje - „neužsakyti komerciniai pranešimai“ (angl. *unsolicited commercial communication*). Nors ES naudojamas terminas lyginant su kitų valstybių to paties reiškinio terminais atrodo siauresnis, tačiau elektroninio pranešimo, skirto tiesioginės rinkodaros tikslams realizavimo formų ES teisės aktuose pripažįstama daugiau. Teismų nuomone, reikia laikytis tokios pozicijos, kad jeigu vartotoją pasiekia pranešimas – pasiūlymas elektroninis laiškas, sms pranešimas, faksimiliniu būdu (naudojant fakso aparatus) atsiųstas pranešimas ar naudojant automatinio skambinimo sistemas be žmogaus įsiterpimo (skambinimo automatus) ir jis yra skirtas tiesioginės rinkodaros tikslams, tai toks pranešimas yra „elektroninis pranešimas, skirtas tiesioginės rinkodaros tikslams“, kitaip - *spam*. Vis dėlto, Lietuvos aukščiausiasis teismas 2001 m. gruodžio 12 d. nutartyje[12] *spam* įvardino kaip „neprašytos komercinio pobūdžio informacijos siuntinėjimas dideliais kiekiais“. Tai pakankamai abstrakti nuostata, kuri yra daug platesnė nei Lietuvos ir ES teisės aktuose pateikiama *spam* samprata.

Australijos įstatymuose vartojamas terminas „neprašyti komerciniai elektroniniai pranešimai“ (angl. *unsolicited commercial electronic messages*“), o ne *spam*. Be to, nėra užuominos netgi apie tai, kad tai turi būti masinis pranešimų siuntimas, netgi priešingai – ir vienas neprašytas komercinis elektroninis pranešimas Australijoje laikomas *spam*. Teismų praktika kol kas (angl. *judicial provision*) šiuo klausimu yra formaliai neutrali, todėl įstatymai galioja visiems nepageidautiems komerciniams elektroniniams pranešimams, nepriklausomai nuo to, kokiu būdu juos gauna vartotojai: elektroniniais laiškais, SMS, MMS ar trumpaisiais pranešimais. Australijos teisės aktuose nurodyta, kad naudojamas terminas „neprašytos komercinės elektroninės žinutės“ neapima faksimilinių ir telefoninio pokalbio metu gaunamų komercinių pranešimų - pasiūlymų. Vis dėlto 2004 metais Britanijos Tautų sandraugos Australijoje generalinis gubernatorius Philip Michael Jeffery, įgaliotas Federalinės vykdomosios tarybos, padarė kelis 2003-čiųjų metų *Spam* akto pakeitimus, kurių vienas -

[10] Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37.
[11] Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1.
[12] LAT CBS teisėjų kolegijos 2001 m. gruodžio 12 d. nutartis c.b. Ž.Budros individuali įmonė „Sėkmės sistema" v. UAB "D.B.S. Ltd.Pte“, Nr. 3K-3-1326/2001 m., kat. 31.4; 37.7; 49.1.

„faksimiliniai pranešimai yra specifinė elektroninių pranešimų rūšis“. Vadinasi, *spam* priskyrė ir faksimiliniu būdu gaunamus pranešimus.[13]

Jungtinių Amerikos Valstijų teisės aktuose *spam* terminas taip pat, kaip ir Lietuvos ar Australijos teisės aktuose, nėra nei vartojamas, nei apibrėžtas. Federalinė prekybos komisija (FPK), kuri yra atsakinga už *spam* reguliuojančių teisės aktų priežiūrą, vartoja terminą „neprašytas komercinis elektroninio pašto pranešimas“ (angl. *unsolicited commercial electronic mail message*). Toks egzistuojantis *spam* apibrėžimas iš pradžių buvo suvokiamas labai siaurai, nes JAV teismų praktikoje pasitaikydavo ne vienas atvejis, kai *spam* buvo siunčiamas ne tik į elektroninį paštą, bet ir, pavyzdžiui, į mobiliuosius telefonus. FPK priėmė naujas taisykles siekiant apsaugoti vartotojus nuo *spam* gavimo į jų bevielius įrenginius, tokius kaip mobiliuosius telefonus (angl. *cellular phone*) ir pranešimų gaviklius. Vis tik FPK minėtas *spam* pasireiškimo formas viename savo pranešimų įvardino kaip *spam* pusbroliais: SPIM - *spam* over instant messaging (liet. spam siunčiamas naudojant pranešimų gaviklius) ir SPIT – *spam* over internet telephony (liet. spam siunčiamas naudojant internetinę telefoniją)[14].

Vis dėlto JAV įstatymų leidėjas, atsižvelgdamas į technologijų augimą bei atkreipdamas dėmesį, kad faksimilinį pranešimą galima siųsti elektroniniu paštu arba naudojantis faksu, Telefonijos Klientų Apsaugos teisės akto (angl. *Telephone Consumer Protection Act – TCPA*) 47 U.S.C. 227 paragrafe nurodė, kad yra nelegalu siųsti nepageidautus masinius komercinius elektroninius pranešimus asmenims, naudojantiems telefonus, faksimilinius aparatus, kompiuterius ar kitus įrenginius.

Be to, pastebėta, kad nors *spam* terminas teisės aktuose ir nevartojamas, tiek Australijos, tiek ir Jungtinių Amerikos Valstijų pagrindiniai teisės aktai, skirti sureguliuoti masinių, komercinių, elektroninių pranešimų siuntimą į elektroninio pašto dėžutes, vadinami ne elektroninių komercinių pranešimų įstatymais ar panašiai, bet *spam* aktais, *spam* įstatymais: Australijoje - „*Spam act of* 2003“, JAV – „*Can-spam act*“.

Argentina yra ta valstybė, kuri *spam* reiškinį reguliuoja pasitelkdama kitų artimų reguliuojamų teisės sričių teisės aktus. Argentinoje pagrindinis įstatymas, kuriuo ginamos elektroninio pašto savininkų teisės gavus *spam*, yra 2000 m. priimtas ir įsigaliojęs Asmens duomenų apsaugos įstatymas (angl. *The Data Protection of Argentina Act*, isp. *La Ley de Protección de Datos Personales).* Šis teisės aktas neapibrėžia *spam* ir nereikalauja, kad elektroninių pranešimų šaltiniai būtų identifikuoti. Be to, aktas nesuteikia teisių IPT blokuoti

[13] Spam regulations 2004, Statutory rules 2004, No. 56 6/04/2004 // http://www.gov.mu/portal/sites/spamweb/download/Spam%20Regulations%202004.pdf; prisijungimo laikas: 2008-10-15.

[14] The Federal Trade Commission. Opening Remarks of Deborah Platt Majoras „Developing A Plan for Action in the Fight Against Malicious Spam“, Spam Summit: The Next Generation of Threats and Solutions, July 11, 2007 // http://www.ftc.gov/bcp/workshops/spamsummit/presentations/Law-Enf.pdf; prisijungimo laikas: 2008-01-30.

spam, kuris jiems taip pat gali sukelti daug materialinės ir nematerialinės žalos, kuri gali pasireikšti ne tik nuostoliais, pelno netekimu, bet ir prestižo praradimu. 2001 m. ir 2004 m. Susisiekimo sekretoriatas (isp. *Secretaría de Comunicaciones)* Argentinos Kongresui bandė pristatyti *anti-spam* įstatymo projektus (isp. *Proyecto de ley de regulación del envío de mensajes de correo electrónico comercial*), kuriuose *spam* įvardijo kaip elektroninio pašto nepageidaujamas komercinis pranešimas – tai visi elektroninio pašto komerciniai pranešimai, kurie siunčiami be išankstinio gavėjo sutikimo arba jei prieš tai nebuvo komercinio ar asmeninio ryšio tarp siuntėjo ir gavėjo. *Spam* sąvoka, pateikta šiame Argentinos *anti-spam* įstatymo projekte, yra labai panaši į JAV teisės suformuluotą sampratą. Projekte taip pat pateikiamas nelegalių elektroninio pašto komercinių pranešimų apibrėžimas: *„tai visi elektroninio pašto komerciniai pranešimai ir nepageidaujami komerciniai pranešimai, kurie neatitinka šio įstatymo keliamų reikalavimų*“. Reikalavimai yra susiję su privalomais elektroninio komercinio pranešimo turinio elementais, komercinių pranešimų siuntimu, kurie bus aptariami 2.2.1 ir 2.2.2 skirsniuose. Argentinos *anti-spam* įstatymo projekte įvardintus nelegalius elektroninio pašto komercinius pranešimus, taip pat kaip ir kitų minėtų valstybių, būtų galima tapatinti su *spam*. Tačiau šiame projekte buvo pamiršti ir neįvardinti faksimiliniu būdu ar judriuoju tinklu siunčiami pranešimai. Greičiausiai dėl to, kad įstatymas buvo per daug griežtas ir nepakankamai išsamus bei aiškus, projektas taip ir nebuvo priimtas ir promulguotas.

Taigi Argentinoje *spam* reguliavimo srityje teisę taikantys subjektai - valstybės institucijos, pareigūnai - yra priversti teisės normas taikyti ne formaliai, o kūrybiškai: renkasi kuo tinkamesnius pagalbos asmeniui įgyvendinti savo teises būdus, imasi veiksmingų teisinio poveikio priemonių, kai reikia apginti asmens teises, įgyvendinti teisingumą, t.y. naudoja ir taiko kitų teisės subinstitutų artimas *spam* reguliavimui teisės normas.

Rusija, kaip ir Argentina, neturi vieno ar kelių konkrečių teisės aktų, kuriuose būtų įvardytas ar apibrėžtas *spam*. 2003 m. UNESCO IFAP (Information for All Programme) Nacionalinio Rusijos komiteto ir Rusijos Federacijos komisijos UNESCO reikalams buvo inicijuotas *anti-spam* projektas. 2006 m. publikuotame *anti-spam* projekto metiniame pranešime „Spam legislation in Russia“ (liet. *spam įstatymai Rusijoje*) *spam* reiškiniui apibūdinti buvo vartojamas *spam* terminas, tačiau šis dokumentas nėra teisės aktas. Egzistuojančiuose ir įsigaliojusiuose teisės aktuose labai neaiškiai apibūdina *spam* pobūdžio pranešimų siuntimą kaip veiką: informacijos, nesuderintos su klientu ar pateiktos kaip tam tikras pasiūlymas ir atsiųstos fiziniam ar juridiniam asmeniui elektroniniu paštu, siuntimas privalo būti nedelsiant nutrauktas. *Anti-spam* projekto metinio pranešimo „Proposed legislation“ skyriuje teigiama, kad „kartu su minėtu projektu buvo atliktos tam tikros Federalinio komunikacijų įstatymo ir Administracinio kodekso pataisos, kurios leidžia suvokti, kad *spam* yra ne tam tikros informacijos rūšis, bet

reiškia informacijos platinimą, pagal kurį siuntėjas tiksliai nežino, kas yra šios informacijos gavėjas“. Įstatymo pataisos rodo tam tikrą Rusijos įstatymų leidybos pažangą, tačiau vis tik šios pataisos nepakankamai aiškiai įvardija, kas yra *spam*. Metiniame pranešime įvardijama, kad elektroniniu ar tradiciniu paštu platinamų pranešimų kūrimas ir siuntimas neidentifikuotiems komunikacinių paslaugų vartotojams yra neleistinas. Šia nuostata siūloma vadovautis kuriant *Anti-spam* įstatymo projektą Rusijoje.

Neformali Rusijos interneto paslaugų teikėjų asociacija OFISP (*Open Forum of the Internet-Service-Providers*) sukūrė interneto vartotojų elgesio kodeksą, kuris netapo Rusijos teisės aktu. Šis kodeksas, pavadintas OFISP – 008, yra dokumentas, sukurtas remiantis verslo taisyklėmis. Šio kodekso 1.1 straipsnyje nurodoma, kad yra *„draudžiamas masinis pranešimų per elektroninį paštą ir kitais asmeninės informacijos keitimosi būdais (įskaitant tokias paslaugas kaip SMS, IRC ir kt.) platinimas, remiantis akivaizdžiai ir vienareikšmiškai išreikšta adresanto iniciatyva“* [15].

Atlikus valstybių teisės aktuose įtvirtintų *spam* apibrėžimų apžvalgą, akivaizdžiai pastebimas vieningos *spam* sąvokos nebuvimas ir skirtingas *spam* termino traktavimas. Vienose valstybėse *spam* sąvoka suvokiama plačiai, pvz., nesuderintos su klientu informacijos siuntimas (Rusija), kitose valstybėse įvardijama ir apibrėžiama daug siauriau – „nepageidaujami elektroniniai komerciniai pranešimai“ (Australija) ar „nepageidaujami komerciniai elektroninio pašto pranešimai“ (JAV). Netgi *spam* platinimo priemonėmis vienur laikoma tik internetas ir mobilusis telefonas, kitur - faksimiliniai aparatai, pranešimų gavikliai ir automatinio skambinimo sistemos be žmogaus įsiterpimo (skambinimo automatai) ar apskritai nėra įvardijama.

Kitas aspektas, kurio pasigendama nagrinėjant valstybių teisės aktus yra tas, jog į sąvokų apibrėžimus nėra įtraukta ne komercinės paskirties elektroniniai pranešimai, kurie yra siunčiami ne rinkodaros tikslais ir ne tam tikrų prekių ar paslaugų reklamai. Nagrinėjant *spam* sampratą buvo įvardinti du *spam* suvokimo aspektai: a) nepageidaujamas elektroninis komercinis pranešimas, kurį naudoja įmonės rinkodaros, marketingo, komerciniais, reklamos tikslais; b) masiškai siunčiamas elektroninis pranešimas, kurio turinys nebūtinai turi būti komercinės paskirties, bet gali būti kenkėjiško, kartais amoralaus pobūdžio ar visiškai beprasmio turinio. Problema yra ta, kad nagrinėjamų valstybių teisės aktuose *spam* apibrėžimas yra siejamas tik su elektroniniais komerciniais pranešimais. Apibrėžimuose pasigendama antrojo *spam* suvokimo aspekto apie elektroninius pranešimus, neturinčius prasmingo turinio ir tik užimančius vietą elektroninio pašto dėžutėje, amoralaus ar piktybinio pobūdžio pranešimus, platinančius įvairius kompiuterinius virusus bei įvairius sukčių platinamus pranešimus. CERT interneto svetainėje pateikta „Symantec“ kompanijos surinkta statistika patvirtina, jog komercinių produktų

[15] Naumov V. Legal aspects of spam in Russia // www.russianlaw.net; prisijungimo laikas: 2008-10-15.

platinimas užima tik 27 proc. visų platinamų *spam* (priedas Nr. 5). Vadinasi, 73 proc. *spam* sudaro kito pobūdžio elektroninės šiukšlės.

2.2 Prievolės elektroniniams komerciniams pranešimams, jų siuntimui bei turiniui:

2.2.1. Elektroninių pranešimų siuntimo metodų *„opt-in“ ir „opt-out“* taikymas, jų trūkumai ir privalumai

Kova prieš *spam* yra sudėtinga ne tik dėl to, kad nėra vieningos *spam* sąvokos, bet ir dėl to fakto, kad neaišku, iš ko susideda neteisėta *spam* platinimo veikla, apimanti didelę *spam* siuntimo būdų įvairovę, kuri priklauso nuo nacionalinių jurisdikcijų. Dėmesio centras, sukėlęs daugybę diskusijų siekiant įtvirtinti *anti-spam* teisę buvo *opt-in* (liet. *sutikimo*) ir *opt-out* (liet. *atsisakymo*) metodų taikymas.

Tai dvi skirtingos *anti-spam* teisės „filosofijos“, kurias nėra sudėtinga suprasti, tačiau sunku priimti vieningą nuomonę ir apsispręsti, kuris metodas yra efektyvesnis. Kiekviena valstybė gina savo poziciją ir laikosi savo teisėje įtvirtinto metodo. Tai nereiškia, kad kažkuris metodas yra netinkamas, tiesiog taikant skirtingus metodus, atsiranda niša plisti elektroniniams pažeidimams, šiuo atveju - *spam* platinimui.

Daugelio valstybių tarp jų Lietuvos, Australijos bei Rusijos teisės aktuose yra įtvirtintas *opt-in* metodas, pabrėžiantis, kad jei vartotojas neišreiškė valios atlikdamas atitinkamus veiksmus gauti komercinio ar kitokio pobūdžio laiškus, vadinasi, tokio laiško vartotojui negalima siųsti. Tai Europos Sąjungos numatyta ir Asmens duomenų ir privatumo apsaugos elektroninių ryšių sektoriuje direktyvos 2002/58/EC 13 straipsnyje įtvirtinta ir 2003 m. spalio 31 dieną įsigaliojusi išankstinė abonento **sutikimo sistema (angl. *opt – in*),** kurios pagrindinė nuostata teigia: *„norint siųsti masinį komercinį elektroninį pranešimą, turi būti gautas išankstinis tokio pranešimo gavėjo sutikimas“*. Vadinasi, adresatas turi duoti leidimą arba aiškiai pareikšti pageidavimą, kad gautų komercinius elektroninius pranešimus. Jeigu toks sutikimas gaunamas, tai terminas *opt-in* turėtų būti suprantamas kaip sutikimas jį gauti „šiuo metu“, „kuriam laikui“ (angl. *„for the time being“*). Tai nėra aiškiai apibrėžiama teisės normose, todėl sutikimas yra trumpalaikės prigimties ir galios, kol klientas pareikš pageidavimą negauti reklaminių komercinių pranešimų, t.y. bus atšauktas. Šis *opt-in* metodas taikomas siunčiant pranešimus faksimiliniais aparatais, mobiliaisiais telefonais ar naudojant automatines skambinimo sistemas.

Direktyvos nuostatos buvo perkeltos į ES valstybių narių nacionalinę teisę, taip pat ir **į Lietuvos** Respublikos teisės aktus, ir jomis yra vadovaujamasi. Apskritai komercinių masinių nepageidaujamų elektroninių laiškų - pranešimų siuntimą ir gavėjų elektroninio pašto duomenų

naudojimą reguliuoja LR elektroninių ryšių įstatymas[16], LR asmens duomenų teisinės apsaugos įstatymas[17], LR reklamos įstatymas[18] ir kiti teisės aktai.

Lietuvoje Elektroninių ryšių įstatymo 68 straipsnio 1 dalis nustato, kad naudoti elektroninių ryšių paslaugas, įskaitant elektroninio pašto pranešimų siuntimą, tiesioginės rinkodaros tikslais leidžiama tik esant išankstiniam abonento sutikimui. Jeigu tokio sutikimo nėra ir vis tiek siunčiamas nepageidaujamas pranešimas (*spam*), tai pažeidžiama minėta įstatymo nuostata. Paminėtina, kad Lietuvoje ne vieną kartą nepageidaujamos komercinės informacijos (arba *spam*) siuntėjai buvo patraukti atsakomybėn. „2004 m. lapkričio 22 d. Valstybinėje duomenų apsaugos inspekcija gavo R.L. skundą dėl nepageidaujamo elektroninio pašto pranešimo. Tyrimo metu nustatyta, kad serveris, iš kurio siųstas nepageidaujamas elektroninio pašto pranešimas, priklauso UAB „Biuro sprendimų tinklas“. UAB „Biuro sprendimų tinklas“ atsakydama į inspekcijos klausimą, pranešė, kad už nustatyto serverio išlaikymą minėtai bendrovei moka ir už jį atsako UAB „Interprekyba“. Inspekcijos darbuotojai minėtoje bendrovėje atliko asmens duomenų tvarkymo teisėtumo patikrą ir nustatė, kad iš UAB „Interprekyba“ pareiškėjui siųstas elektroninio pašto pranešimas tiesioginės rinkodaros tikslu be išankstinio abonento sutikimo, taip pažeista Elektroninių ryšių įstatymo 68 straipsnio 1 dalis.“[19] Šio įstatymo 68 straipsnio 2 dalis numato, kad asmuo, kuris teikdamas paslaugas ar parduodamas prekes Asmens duomenų teisinės apsaugos įstatymo nustatyta tvarka ir sąlygomis gauna iš savo klientų elektroninio pašto kontaktinius duomenis, gali naudoti šiuos kontaktinius duomenis savo paties panašių prekių ar paslaugų rinkodarai, jei klientams yra suteikiama aiški, nemokama ir lengvai įgyvendinama galimybė nesutikti arba atsisakyti tokio kontaktinių duomenų naudojimo pirmiau nurodytais tikslais, kai šie duomenys yra renkami ir, jei klientas iš pradžių neprieštaravo tokiam duomenų naudojimui, siunčiant kiekvieną žinutę. Vadinasi, šia nuostata Lietuvos įstatymai iš dalies įtvirtina ir kitą metodą – **atsisakymo (angl. *opt-out*)**, kuris reiškia, kad be išankstinio asmens sutikimo galima naudoti asmens duomenis ir siųsti elektroninius komercinius pranešimus iki to momento, kol asmuo pareikš atsisakymą daugiau nebenaudoti jo asmens duomenų (pvz., vardo, pavardės, el. pašto adreso ar mobilaus telefono numerio) ir nebesiųsti šių elektroninių komercinių pranešimų. Tačiau atkreiptinas dėmesys, kad šis *opt-out* metodas pagal Lietuvoje galiojančius įstatymus taikomas tik tuomet, jei kartą jau buvo išreikštas sutikimas tam pačiam duomenų valdytojui naudoti asmens kontaktinius duomenis ir gauti elektroninius komercinius pranešimus panašių prekių ar paslaugų rinkodarai. „Elektroninių ryšių įstatymo nuostatos iš esmės atkartoja Direktyvos dėl privatumo ir elektroninių ryšių, kurią šis įstatymas ir

[16] LR elektroninių ryšių įstatymas (Žin., 2004, Nr. 69-2382).
[17] LR asmens duomenų teisinės apsaugos įstatymas (Žin., 2003, Nr. 15-597).
[18] LR reklamos įstatymas (Žin., 2000, Nr. 64-1937).
[19] M. Kiškis, R. Petrauskas, I. Rotomskis ir kt. Teisės informatika ir informatikos teisė: vadovėlis. - Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006. P. 125

įgyvendina, nuostatas. Elektroninių ryšių įstatyme keliamas vienas svarbus reikalavimas bet kokia reklamai, pateikiamai elektroninių ryšių priemonėmis, tam reikia išankstinio abonento sutikimo. Pavyzdžiui, siekiant perduoti reklamą telefonu, tokio sutikimo galėtų būti atsiklausiama prieš pradedant sakyti reklaminio pranešimo tekstą, arba prieš siunčiant faksą su reklaminiu tekstu galima atsiklausti telefonu dėl sutikimo gauti reklaminį pranešimą faksu. Tačiau kai kuriais atvejais gauti tokį sutikimą gali būti kiek sudėtingiau. Pavyzdžiui, būtų gana sudėtinga gauti abonento sutikimą prieš išsiunčiant reklaminį tekstą trumpąja SMS žinute: atsiklausti dėl žinutės siuntimo paskambinus telefonu būtų itin neracionalu. Tačiau abonento sutikimą dėl reklaminės informacijos siuntimo jam trumposiomis SMS žinutėmis būtų galima gauti, kai abonentas įsigydamas prekę ar paslaugą, duoda sutikimą dėl tam tikros reklamos jam siuntimo, pasirašydamas kokias nors lojalumo programos sąlygas ir pažymėdamas tam tikrą laukelį, reiškiantį sutikimą dėl reklaminių SMS žinučių siuntimo.“ [20]

Australijoje, lyginant su kitomis pasaulio valstybėmis**,** yra priimta nemažai teisės aktų, reguliuojančių elektroninių pranešimų siuntimą - tai 1997-ųjų metų Telekomunikacijų įstatymas (angl. *Telecommunications Act of 1997*) bei 1974 metų Australijos prekybos įstatymas (angl. *Trade Practices Act of 1974*). Australija**,** priešingai nei Lietuva, Rusija, Argentina, yra viena iš tų valstybių, kuri savo nacionalinėje teisėje priėmė specialųjį teisės aktą, skirtą *spam* srities reguliavimui – tai 2003 metų *Spam* aktas (angl. „*Spam act of 2003*“). Šiame akte išsamiai apibrėžiama, kas yra elektroniniai (komerciniai) pranešimai, numatyti konkretūs reikalavimai siunčiamiems elektroniniams komerciniams pranešimams, aiškiai nustatytos ribos tarp pageidaujamų ir nepageidaujamų elektroninių komercinių pranešimų. Šiame Australijos teisės akte „Spam act of 2003” yra įtvirtinta nuostata dėl ***opt–in*** **metodo**, kurioje numatyta, jog „draudžiama siųsti ar liepti siųsti komercinius elektroninius pranešimus, kurie turi Australijos nuorodą[21] (angl. *Austalian link*) ir kurie nėra paskirtieji komerciniai elektroniniai

[20] L. Markauskas. Reklamos teisinis reglamentavimas: teorija ir praktika. – Vilnius: UAB „Mokesčių srautas“, 2008. P. 159

[21] Remiantis teisės akto „Spam act of 2003” 7 straipsniu laikoma, kad komerciniai elektroniniai pranešimai turi Australijos nuorodą, jei 1) pranešimas buvo sukurtas ir išsiųstas Australijoje; 2) individas pranešimo siuntimo metu fiziškai yra Australijoje arba pranešimo siuntimo metu organizacijos centrinė administracija ir valdyba, yra Australijoje; 3) kompiuteris ar serveris ar kitas įrenginys, kuris yra naudojamas prisijungimui, yra lokalizuotas Australijoje; 4) kai elektroninio pašto savininkas reziduoja Australijoje, kai pranešimas yra gaunamas į jo pašto dėžutę (jei tai fizinis asmuo, tai fiziškai yra Australijoje, jei tai juridinis asmuo, tai jo buveinė ir pagrindinė veikla turi būti vykdoma Australijoje); 5) jei pranešimas negali būti pristatytas, nes elektroninis pašto adresas neegzistuoja – laikantis nuomonės, kad toks elektroninio pašto adresas galėtų egzistuoti kaip toks ir tokiu atveju pranešimas pasiektų elektroninio pašto dėžutę naudojant kompiuterį, serverį ar kitą įrenginį, lokalizuotą Australijoje.

pranešimai[22]. Šiai nuostatai minėtas draudimas netaikomas: *a) jei pranešimo gavėjas išreiškė išankstinį sutikimą (angl. consent) dėl pranešimų siuntimo; b) jei asmuo nežinojo ar negalėjo išsiaiškinti, kad pranešimas turi Australijos nuorodą; c) jei asmuo, siuntęs pranešimą ar liepęs siųsti pranešimą, suklydo ir tai padarė per klaidą.*

Australijos specialaus teisės akto nuostatos norma, skirtingai nei Lietuvos įstatymuose, formuluojama per imperatyvios draudžiamosios teisės normos prizmę, aiškiai nurodant, jog yra „draudžiama siųsti elektroninius komercinius pranešimus“. Įstatymas opt-in metodą įgyvendina per vieną iš suformuluotos normos dispozicijos išimčių - nuostata netaikoma, „jei pranešimo gavėjas išreiškė išankstinį sutikimą“. Australijos teisės akto 2 priede yra išaiškinta, kas yra laikoma pranešimo gavėjo sutikimu. Šiame akte sąvoka asmens ar organizacijos „sutikimas“, „leidimas“, reiškia: *„a) išreikštą sutikimą (angl. express consent) ar b) pagrįstą/natūralų sutikimą, kuris dažnai susiklosto tarp fizinių asmenų ar organizacijų, kuriuos sieja verslo ar kitokie ryšiai.*“ „Išreikštas sutikimas“ praktikoje dažniausiai įgyvendinamas, kai asmuo užsiregistruoja tam tikroje interneto svetainėje ir nurodo raštu ar pažymi varnele, jog pageidauja gauti ar neprieštarauja, jog bus siunčiami tam tikri komerciniai elektroniniai pranešimai į jo elektroninį paštą, mobilųjį telefoną ar kitą įrenginį. Įstatymas numato, kad elektroniniai komerciniai pranešimai bus siunčiami iki to momento, kol asmuo atšauks savo sutikimą, kuris privalo įsigalioti per 5 darbo dienas, skaičiuojant terminą nuo tada, kai elektroninis pranešimas – atsisakymas buvo išsiųstas individui ar organizacijai.

Australijos įstatymų leidėjas priėmė svarbias ir tik šioje valstybėje taikomas teisės normas dėl viešai prieinamų elektroninio pašto adresų, kurių viešinimas kitose valstybėse *spam* atžvilgiu tampa problema. Ši sritis nei Lietuvoje, nei Rusijoje, nei Argentinoje, nei JAV nėra reglamentuota. Šiomis teisės normomis Australijos teisėje iš dalies įgyvendinamas ne tik *opt-in*, bet ir *opt-out* metodas. Australijos teisės akto 2 priedo 4 punktas nurodo, kad „*jei elektroninio pašto savininko adresas yra viešai prieinamas ar publikuojamas, tai dar nereiškia, kad yra duodamas elektroninio pašto savininko sutikimas elektroninių komercinių laiškų siuntimui.*“ Įstatymas numato išimtis – esant, išskirtiniam paviešinimui: *„elektroninis adresas įgalina visuomenę ar dalį visuomenės siųsti elektroninius pranešimus: a) tam tikram tarnautojui ar darbuotojui; b) tam tikram direktoriui ar tam tikros organizacijos atstovui; c) tam tikram verslo partneriui; d) tam tikram statutiniam tarnautoju; e) asmeniui, kuris tuo metu eina, užima ar*

[22] Vadovaujantis Australijos akto „Spam act of 2003”6 straipsniu ir priedu Nr.1 paskirtųjų elektroninių komercinių pranešimų (angl. *designated commercial electronic messages*) sąvoka skiriasi nuo tradicinės elektroninių komercinių pranešimų sąvokos. Paskirtieji elektroniniai komerciniai pranešimai – tai valstybės institucijų, registruotų politinių partijų, religinių organizacijų, labdaros įstaigų savo nariams siunčiami elektroniniai pranešimai, susiję su šios organizacijos prekių ir paslaugų tiekimų. Taip pat šiai sąvoka priskiriami ir švietimo įstaigų siunčiami paskirtieji elektroniniai komerciniai pranešimai savo nariams, darbuotojams, pvz., studentams, turintiems universiteto domeno vardu sukurtą elektroninio pašto dėžutę, siunčiami universiteto, studentų atstovybės ar bibliotekos paskirtieji elektroniniai komerciniai pranešimai.

vykdo tam tikras pareigas ar tam tikrą poziciją tam tikroje įstaigoje ar organizacijoje; f) asmuo ar asmenų grupė, kuri tuo metu vykdo tam tikras funkcijas ar atlieka tam tikrą svarbų vaidmenį organizacijoje - jei šis elektroninio pašto adresas buvo išskirtinai viešai publikuotas, jei buvo publikuotas su direktoriaus ar aukštesnio rango valstybės tarnautojo, ar organizacijos vadovo, ar partnerio žinia bei siunčiamas pranešimas nurodytu elektroniniu adresu yra susijęs tiek, kiek atitinkamas asmuo atlieka jam pavestas funkcijas, darbus ar pareigas“[23]. Taigi, kaip matyti, ne tik Lietuvoje, bet ir Australijoje yra išimtinai taikomas *opt-out* metodas.

Šiame Australijos teisės akte, lyginant su Lietuvos įstatymais, *opt-in* metodo principas yra tas pats, tačiau ši teisės norma yra daug platesnė ir išsamesnė siekiant sureguliuoti *spam* sritį. Šioje normoje įvardijamos veikos, „draudžiančios siųsti“ ar „liepti siųsti“, atskiria atsakomybės taikymą pavaldiniui ir jo vadovui.

Iš kitos pusės *opt-out* metodas taikomas verslo srityje, kai tarp verslo partnerių egzistuoja verslo ryšiai, jie gali siųsti vienas kitam elektroninius komercinius pranešimus be išankstinio sutikimo. Tačiau būtina pranešimų siuntimą nutraukti, jei bent kartą buvo to paprašyti.

Remiantis Jungtinių Tautų konferencijos dėl prekybos ir jos vystymo (UNCTAD) 2003 e-komercijos ir jos plėtojimo pranešimu, pastaruoju metu apie 58 proc. viso pasaulio *spam* yra sukuriama JAV. Todėl yra suprantama, kad lyginant su likusia pasaulio dalimi, JAV turi vieną didžiausių interesų sukurti veiksmingą *anti-spam* įstatyminę bazę. Lyginant su jau nagrinėtomis valstybėmis (Lietuva ir Australija), JAV taiko šiek tiek kitus būdus ir metodus kovai prieš spam. Jungtinių Valstijų prezidentas 2003 m. gruodžio 16 d. pasirašė *Can Spam Act* of 2003 aktą, kuris įsigaliojo 2004 m. sausio 1 d. Pagrindinis šio akto tikslas yra reguliuoti valstijų prekybos santykius, nustatant kartu tam tikrus apribojimus bei sankcijas dėl siunčiamų nepageidaujamų komercinių elektroninių pranešimų internetu. 2003 metų *Can spam* aktas atskiria masiškai siunčiamą *spam* nuo teisėtų komercinių elektroninių pranešimų siuntimo bei taiko ***opt-out*** **atsisakymo metodą.** Žinoma, kad ne tik JAV, bet ir tokiose valstybėse, kaip Japonija, Kanada, Singapūras, Argentina, Pietų Korėja, Portugalija, taikančiose *opt-out* metodą, teisės aktuose yra nustatyta, kad pranešimų siuntėjas gali siuntinėti elektroninius pranešimus elektroninio pašto savininkams be jokio išankstinio sutikimo, netgi nesant jokiems išankstiniams verslo ryšiams, ir net jei gavėjas nėra pasirinkęs iš anksto gauti atitinkamus pranešimus. Tačiau pranešimų siuntėjas privalo sąžiningai suteikti galimybę gavėjams atsisakyti gaunamų pranešimų ir būti pašalintiems iš siuntėjo siunčiamų pranešimų sąrašų. JAV teisėje taikomo *opt-out* metodo esmė ta, kad įstatymas numato teisę siųsti elektroninius pranešimus, kol gaunantis asmuo šių

[23] Spam act of 2003, Schedule 2 – Consent, 4 punktas „When consent may be inferred from publication of an electronic address” .

pranešimų atsisakys arba jei siunčiami pranešimai neatitiks 2003 metų *Can spam* akte numatytų reikalavimų siunčiamiems komerciniams elektroninio pašto pranešimams, pvz., nebus nurodyti siuntusio pranešimą asmens identifikaciniai duomenys.

Telefonijos Klientų Apsaugos teisės akte yra įtvirtinta nuostata, kad „*yra nelegalu siųsti asmenims, naudojantiems telefonus, faksimilinius aparatus, kompiuterius ar kitus įrenginius, nepageidautus reklaminius pranešimus į minėtus įrenginius, kurie yra pritaikyti siųsti nepageidautus masinius komercinius elektroninius pranešimus*“ [24]. Darytina išvada, kad JAV teisėje galioja ir *opt-in* taisyklė faksimiliniu būdu siunčiamiems komerciniams pranešimams, nes siųsti faksu nepageidautus komercinius elektroninius pranešimus yra neteisėta.

Vis dėlto verslo elektroniniam susirašinėjimui yra taikoma *opt-out* metodas. 2005 m. buvo priimtas Faksu gaunamų šiukšlių prevencinis aktas (angl. *The Junk Fax Prevention Act of* 2005), kuris įsigaliojo 2005 m. liepos 9 d. Šis aktas leidžia verslininkams siųsti nepageidaujamus faksimilinius pranešimus verslo partneriams, tarp kurių yra susiklostę verslo ryšiai. „Susiklostę verslo ryšiai“ suprantami, kaip „*iš anksčiau susiformavę ar esamuoju laiku besiformuojantys savanoriški abiejų pusių komunikacija pagrįsti santykiai tarp pavienių asmenų ar bendrovių ir abonentų nepriklausomai nuo to, ar davė vieni kitiems patvirtinimus, pagrįstus pasiteiravimu, prašymu, perkant ar įsigyjant tam tikras prekes ar paslaugas, ir susiklostęs santykis nebuvo anksčiau nutrauktas nei vienos šalies*.“ Tačiau visada turi egzistuoti tokių pranešimų atsisakymo teisė.

Po *Can spam* teisės akto įsigaliojimo pasaulyje pasirodė įvairaus pobūdžio straipsnių apie šioje supervalstybėje taikomą teisės aktą, jo privalumus ir trūkumus. Konstatuojama, kad priėmus Can spam teisės aktą, statistiškai mažėja nepageidaujamų elektroninių laiškų kiekis. Dar geresnių rezultatų būtų galima pasiekti, jei pavyktų užkirsti kelią trečiųjų kompiuterių sistemų naudojimą *spam* siuntimui. Šitas teisės aktas reikalauja visų pranešimų turėti *opt-out* funkciją, draudžia naudotis atvirais *proxy*[25] serveriais arba nurodyti neteisingas elektroninių komercinių pranešimų antraštes. Vis tik naujasis JAV įstatymas gali nesustabdyti *spam*. Didžiausią susirūpinimą kelia tai, kad leidžiama *spam* siuntėjams siųsti *spam*. Todėl IT specialistai bus priversti ir toliau naudoti *anti- spam* filtrus ir blokuoti legaliai (teisės aktai nedraudžia) siunčiamus, bet nepageidaujamus elektroninius laiškus.

2004 metų „Spam ir įstatymas“ konferencijoje San Franciske buvo išsakyti keli neigiami komentarai dėl federalinio *Can spam* akto efektyvumo. Techninės ir teisinės srities

[24] *Telephone Consumer Protection Act* – 47 U.S.C. 227 paragrafas.

[25] Proxy serveris yra tarpinis serveris tarp kompiuterio ir svetainės, kurią norima pasiekti, serverio. Jie naudojami tam, kad būtų galima paslėpti vartotojo IP adresą, t.y. naršant per internetinius tinklapius, teikia anoniminio naršymo paslaugą. kurios dėka praktiškai yra neįmanoma nustatyti naudojamo kompiuterio buvimo vietos. Naudotis *proxy* serveriais legaliais tikslais nėra draudžiama. Dažniausiai *proxy* serveriai naudojami apeiti įvairius apribojimus mokyklose, darbovietėse, nesivarginti dėl prieigos apribojimo vartotojo IP adresui ar geografiniam regionui ar kt.

specialistai, kvestionavo federalinės vyriausybės sugebėjimus įgyvendinti šituos apribojimus ir kritikavo tai, kad šis teisės aktas išstumia griežtesnius, šiuo atžvilgiu valstijose galiojančius teisės aktus.

Argentina, kaip ir JAV, savo teisėje laikosi ***opt-out*** metodo. Argentina, kaip jau minėta, yra viena iš tų valstybių, kuri rengia specialiuosius teisės aktų projektus dėl ***spam.*** Šiuo metu ***spam*** teisinis reguliavimas įgyvendinamas per Argentinos asmens duomenų apsaugos įstatymą. Paminėtinas 27 straipsnis „Duomenų failai, registrai ir duomenų bazės reklamos tikslams“, kuriame nurodyta, kad „***duomenys gali būti renkami ir yra tinkami naudoti tam tikrais reklamos, komerciniais ar rinkodaros tikslais ir gali būti prieinami/kaupiami tam tikrų juridinių asmenų adresų rinkmenose, dokumentų platinimui, reklamai, tiesioginiams išpardavimams ar kitai panašiai veiklai. Savininkas, remdamasis šiuo straipsniu, turi teisę bet kuriuo metu pareikšti atsisakymą*** (angl. ***request withdrawal***) ***ar blokuoti savo vardu tokių duomenų, kurie yra kaupiami duomenų bazėse, naudojimą***“. Taigi, kaip matyti, Argentinos teisėje, priešingai nei Lietuvoje, JAV ar Australijoje, nėra konkrečių ar specialių teisės aktų ar teisės normų, siekiant sureguliuoti ***spam***. Lyginant su kitomis valstybėmis, šiame teisės akte nėra numatyta, kokiais būdais atsisakymas turėtų būti įgyvendinamas, ar visuomet turėtų būti taikomas tik ***opt-out*** metodas, ar atsisakantysis vykdydamas atsisakymo procedūrą nepatirs tam tikrų išlaidų. Apskritai Argentinos teisėje nėra numatyta, ar įstatymas apima ir elektroninę erdvę. Vis tik Argentinoje taikomo ***opt-out*** metodo atžvilgiu galima teigti, kad Argentinos įstatymų leidėjas šią sritį reguliuoja per asmens duomenų teisinės apsaugos įstatymo nuostatas. Šiuo atžvilgiu analizuojant ***spam*** per asmens duomenų apsaugos prizmę, tikėtina, kad asmens duomenimis laikomas ir elektroninio pašto adresas. Asmuo nesutinkantis, kad būtų naudojami jo asmens duomenys, turi teisę pareikalauti duomenų valdytojo (šiuo atžvilgiu siuntėjo) pašalinti jo duomenis iš kaupiamų duomenų registro, o duomenų valdytojas (komercinių pranešimų siuntėjas) turi šią pareigą vykdyti. Argentinos teismai vadovaudamiesi minėtu teisės aktu jau nuo 2003 matų lapkričio 11 d. sprendžia ***spam*** bylas. Viena pirmųjų su ***spam*** susijusi byla ir buvo dėl ***opt-out*** metodo pažeidimo. Federalinis Buenos Aires teismo teisėjas suformavo precedentą dėl ***spam***. Ieškovai, Gustavo Daniel Tanus ir Pablo Andres Palazzi, du nacionaliniai asmens duomenų apsaugos teisės ekspertai, pareiškė ieškinį Argentinoje gerai žinomam ***spameriu***i dėl jų teisių pažeidimo pagal Asmens duomenų apsaugos įstatymo 27 straipsnį. Ieškovai kaltino, kad minėta įstatymo nuostata suteikia teisę atsisakyti gauti pranešimus, tačiau atsakovas nepatenkino jų prašymų pašalinti jų duomenis (t.y. elektroninio pašto adresus) iš savo duomenų bazės. Šios bylos nagrinėjimas tęsėsi visus metus teisėjui diskutuojant dėl jurisdikcijos klausimų, t.y., kuris teisėjas turėtų nagrinėti šią bylą: federalinio teismo teisėjas ar komercinės teisės teisėjas. Galiausiai federalinis apeliacijų teismas nusprendė, kad federalinis teismas turi pareigą nagrinėti

šią bylą vadovaujantis tuo, kad buvo naudojamas internetas *spam* siųsti, ir tai nėra tik komercinės teisės nagrinėtinas objektas. Teisėjas, remdamasis Argentinos asmens duomenų apsaugos įstatymo 1,2, 5, 11 ir 27 straipsniais, nusprendė, kad pranešimų siuntimo proceso metu kaltinamasis turėjo susilaikyti nuo papildomų elektroninių laiškų siuntimo ieškovams po to, kai buvo pareikštas prašymas daugiau nebesiųsti. Teisėjas taip pat byloje akcentavo, kad taip pat yra draudžiamas elektroninio pašto duomenų perleidimas tretiesiems asmenims[26]. Taip buvo sukurtas pirmasis Argentinos precedentas, nagrinėjant *spam* bylą dėl *opt-out* metodo, vadovaujantis Argentinos Asmens duomenų apsaugos įstatymo nuostatomis.

Opt-out metodą taikančiose šalyse yra ypač populiarūs *nespamo* (angl. „*Do-not-spam*“) registrai, į kuriuos savo elektroninio pašto adresus įtraukę asmenys deklaruoja savo valią, jog jie nepageidauja gauti elektroninių komercinių pranešimų. Į šiuos sąrašus elektroninės reklamos platintojai turėtų atsižvelgti prieš siųsdami elektroninius komercinius pranešimus. Tačiau daugelis *spamerių*, kurie jau dabar pažeidinėja *anti-spam* įstatymus ir ignoruoja reikalavimus nesiųsti *spam* elektroninio pašto adresais, kurie yra *nespamo* duomenų bazėje. *Spameriai* gali net pasinaudoti šiuo registru, kaip šaltiniu gauti galiojančius elektroninio pašto adresus tolimesniam *spam* siuntinėjimui.

Kaip jau pastebėta analizuojant *spam* sąvokos apibrėžimą, **Rusijos Federacijoje** nėra aiškaus teisinio reguliavimo ir dėl nepageidaujamų elektroninių laiškų siuntimo, nors jau 2004 metų balandžio 30 d. EBPO (angl. OECD) parengtoje ataskaitoje ne EBPO valstybėms narėms „Spam legislation“ skyriuje apie Rusijos Federaciją nurodyta, kad ši valstybė savo nacionalinėje teisėje pripažįsta ir taiko ***opt-in* metodą**. Federalinio komunikacijų įstatymo (angl. *Federal Law 'On Communication'*) Nr. 126-FZ 62 straipsnyje numatyta, kad „*komunikacinių paslaugų vartotojas turi teisę siųsti, gauti ar atsisakyti pranešimų gavimo*“. Vadinasi, Rusijos įstatymas numato galimybę vartotojams atsisakyti gauti tam tikrus pranešimus, tačiau įstatymų leidėjas nenurodo atsisakymo sąlygų. Remiantis šia nuostata, būtų galima teigti, kad Rusijos nacionalinėje teisėje veikiau yra įtvirtintas atsisakymo *opt-out* metodas nei *opt-in*. Vis dėlto Elektroninės komercijos (angl. „*On electronic Commerce*“) įstatymo 18 straipsnio 4 punkte yra suformuluota teisės norma, kuri iš dalies ir įgyvendina opt-in metodą ir iš dalies įvardija, kada draudžiama siųsti elektroninio pašto savininkui nepageidaujamus elektroninius pranešimus: „*informacijos, nesuderintos su klientu ar pateiktos kaip tam tikras pasiūlymas ir atsiųstos fiziniam ar juridiniam asmeniui elektroniniu paštu, siuntimas neabejotinai ir nedelsiant privalo būti nutrauktas*“ (angl. *determined*). Kalbant apie teisėje taikomą *opt-in* metodą, reikalaujama išankstinio sutikimo. Rusijos Federaciniame komunikacijų įstatyme, kitaip nei jau analizuotų

[26] Data protection law and spam. First spam case in Argentina // http://www.habeasdata.org/SpamEnglish; prisijungimo laikas: 2008-05-25.

valstybių įstatymuose, kalbama ne apie išankstinį elektroninio pašto savininko sutikimą, o informacijos suderinamumą su klientu. Įstatyme taip pat nėra paaiškinta, kokiu būdu turėtų būti informacija derinama su klientu. Iškilus teisiniam ginčui tarp teisinio santykio dalyvių, toks teisės aktas galėtų būti įvairiai interpretuojamas, todėl būtų pažeistas teisingas, tikslus ir vienodas teisės normų prasmės supratimas ir taikymas.

Iš 5 nagrinėtų šalių, reguliuojančių elektroninių komercinių pranešimų siuntimą, vienos laikosi *opt-in*, kitos – *opt-out* metodo, tačiau kuris yra veiksmingesnis metodas sunku nustatyti. Kaip jau pastebėta, valstybės priverstos daryti išimtis. Pavyzdžiui, ne visos ES valstybės narės pasirinko *opt-in* metodą, numatytą ES direktyvose. Belgija ir Portugalija taiko *opt-out* sistemas, kurios galioja siųsti pranešimus ir individams, ir organizacijoms. Suomija įtvirtina *opt-in* sistemą individams, o *opt-out* – organizacijoms. JAV irgi nėra vieningai laikomasi *opt-out* metodo. Pvz., kalbant apie komercinius pranešimus, Kalifornija juos apibrėžia kaip komercinę elektroninio pašto reklamą (angl. *Commercial e-mail advertisement*) (straipsnis 1.8. 2003, paragrafas 14529.1). Įstatymas reikalauja, kad pageidaujant gauti šiuos pranešimus būtų pareikštas tiesioginis sutikimas. „Tiesioginis sutikimas“ reiškia, kad gavėjas turi išreikšti sutikimą gauti elektroninio pašto reklamas iš reklamuotojo. (Article1.8, 2003, paragrafas 17529.1). Vadinasi, Kalifornijos valstijoje yra taikomas *opt-in* metodas.

Spam teisinio reguliavimo kritikai, atkreipdami dėmesį į nepageidaujamus elektroninius pranešimus, teigia, kad teisės aktai yra skirtingi (*opt-in* prieš *opt-out*), jie nepadės kontroliuoti *spam* augimo. O valstybės, turėdamos laikytis jurisdikcijos taisyklių, bando traukti atsakomybėn ir už jų ribų esančius *spamerius*, tačiau yra bejėgės tai padaryti. Joms netgi sunku nustatyti *spamerių* buvimo vietą, kadangi daug *spam* atsiunčiama iš kitų šalių. Todėl manoma, kad tokie teisės aktai neišspręs *spam* problemos.

2.2.2. Teisės aktų reikalavimai elektroninių komercinių pranešimų turiniui ir jų elementams

Šiuo metu vis didesnę reikšmę įgyja internetu platinama reklama, kuria norima, pasipelnyti verčiant vartotoją rinktis prekes ir paslaugas, siekiant sukurti rinką elektroninėje erdvėje. Daugelis valstybių yra priėmusios teisės normas, reguliuojančias elektroninių komercinių pranešimų turinį ar kitus privalomus elementus, norint apsaugoti vartotojus nuo nepageidaujamų elektroninių pasiūlymų. Vienas iš reikalavimų, kuriuo siekiama apsaugoti vartotojo interesus -nesudėtinga ir nemokama nepageidaujamo pranešimo atsisakymo sistema. Kiekviename elektroniniame pranešime turėtų būti tam tikra pranešimo atsisakymo galimybė, kuri praktiškai būtų įgyvendinama įdiegus **„atsisakymo“ funkciją (angl. „*unsubscribe*“).**

Lietuvos Elektroninių ryšių įstatyme yra įtvirtinta nuostata, kad vartotojams, kurių asmens duomenys, tarp jų ir elektroninio pašto adresas, naudojami tiesioginės rinkodaros tikslais, turi būti suteikiama aiški ir lengvai įgyvendinama galimybė nemokamai ir paprastomis priemonėmis nesutikti su savo elektroninių kontaktinių duomenų naudojimu. Vadinasi, klientas visuomet turi turėti teisę atsisakyti gauti elektroninius komercinius pranešimus ir ši teisė turi būti lengvai įgyvendinama, vartotojui nepatiriant jokių finansinių išlaidų. Elektroninių ryšių įstatymo 68 straipsnio 3 dalyje nurodomi kiti reikalavimai, kitaip tariant, būdai, kuriais būtų galima įgyvendinti atsisakymo teisę: *„draudžiama tiesioginės rinkodaros tikslu siųsti elektroninio pašto pranešimus slepiant siuntėjo, kurio vardu informacija siunčiama, tapatybę arba nenurodant galiojančio adreso, kuriuo gavėjas galėtų pareikalauti nutraukti tokios informacijos siuntimą“*. Taigi vadovaujantis minėtomis nuostatomis, norint atsisakyti siunčiamų pranešimų, Lietuvos įstatymas numato dvi konkrečias alternatyvas: arba nurodyti siuntėjo tapatybę, arba galiojantį adresą. Tačiau reikėtų suprasti, kad siuntėjas gali ir nenurodyti atgalinio adreso, jeigu nurodo savo tapatybę. Tačiau įstatyme nėra paaiškinta, kas yra „tapatybė“, kokie privalomi tapatybės rekvizitai, kai pranešimą siunčia fizinis ir juridinis asmuo.

Lyginant su kitų valstybių teisės aktais, daugelyje jų atgalinio adreso ir identifikavimo duomenų įtraukimas yra privalomas. Pavyzdžiui, Australijos 2003 m. akte dėl *spam* formuluojama aiški ir konkreti taisyklė, jog „komerciniai elektroniniai pranešimai turi turėti funkciją „atsisakyti“ (angl. *unsubscribe*)“. Australijos įstatymų leidėjas nustato prievolę įtraukti į elektroninį pranešimą tam tikrus sudėtinius elementus ir pateikia juos imperatyvios draudžiamosios normos išimtyje: *„asmeniui draudžiama siųsti ar versti kitą asmenį siųsti elektroninius komercinius pranešimus, kurie turi australišką nuorodą ir kurie nėra priskirtieji komerciniai elektroniniai pranešimai, išskyrus, jei*

a) į pranešimą yra įtrauktas trumpas pareiškimas (angl. statement) apie tai, kad gavėjas turi teisę naudoti pranešime esantį individo ar organizacijos elektroninį adresą, kuriuo būtų galima atsisakyti siunčiamų pranešimų ar naudoti kitoms panašaus pobūdžio reikmėms;

b) pareiškimas yra aiškiai ir lengvai pastebimas;

c) elektroninis adresas bent 30 dienų nuo siuntėjo pranešimo išsiuntimo gavėjui yra veikiantis ir priima gavėjų siunčiamus pranešimus - atsisakymus (jei tokių būtų) bei panašaus pobūdžio kitus gavėjų siunčiamus pranešimus;

d) elektroninis adresas yra teisėtai įgytas;

e) elektroninis adresas tenkina sąlygą ar sąlygas, numatytas įstatyme.

Minėtos nuostatos negalioja, jei asmuo nežinojo ar stengdamasis sužinoti negalėjo išsiaiškinti, kad pranešimas turi Australijos nuorodą. Šios įstatymo sąlygos galioja tiek, kiek nebuvo susitarta dėl terminų ir sąlygų sutartyje ar susitarime tarp pranešimą siuntusio individo

ar organizacijos ir elektroninio pašto savininko. Ši norma negalioja, jei asmuo suklydo siųsdamas ar liepęs siųsti pranešimą. Tačiau jei siuntėjas nori remtis šia nuostata, jam privalu įrodyti nežinojimo faktą“

Nepaisant to, kad Australijos įstatymo leidėjas gana tiksliai apibrėžė atsisakymo funkcijos įgyvendinimo mechanizmą (lengvai pastebimas atgalinis adresas, jo 30 dienų galiojimo terminas, atsisakymo funkcijos egzistavimas), norint siųsti elektroninį komercinį pranešimą, skirtingai nei Lietuvos įstatymai, jis numato ne alternatyvą, o 17 straipsnyje reikalauja įtraukti ir kitą privalomą elektroninio komercinio pranešimo elementą - tikslią informaciją apie pranešimo siuntėją:

Asmenims draudžiama siųsti ar liepti siųsti komercinius elektroninius pranešimus, kurie turi australišką nuorodą, išskyrus įgyvendinant visas čia išdėstytas sąlygas: a)pranešime galima aiškiai ir tiksliai identifikuoti asmenį ar organizaciją, kurie siuntė pranešimą; b)pranešime yra įtraukta tiksli informacija apie tai, kaip gavėjas gali greitai sukontaktuoti su individu ar organizacija, siuntusiais pranešimą; c) ta informacija patenkina sąlygą ar sąlygas (jei tokių yra) apibrėžtas įstatyme; d)ši informacija turi būti tinkama ir galiojanti dar 30 dienų po pranešimo išsiuntimo.

Panašiai ir JAV *spam* akto 5 dalyje nurodoma, kad *„...(3) yra privalomas atgalinio adreso įtraukimas...“ ir „...(5) privalomas identifikavimo duomenų, atsisakymo (opt-out) teisės ir fizinio adreso įtraukimas į pranešimą.*“

U.S.C. 7704 (a) (3)(A) pateikia, kad „*Yra neteisėta bet kuriam asmeniui į apsaugotą kompiuterį inicijuoti siuntimą/perdavimą komercinių elektroninio pašto pranešimų, kurie nepateiktų funkcionuojančio atgalinio elektroninio pašto adreso ar kito Internetu paremto mechanizmo, kuris aiškiai ir pastebimai vaizduotų, kad (i) gavėjas gali naudoti jį kaip būdą, apibrėžtą pranešime, ir atgalinį elektroninio pašto pranešimą ar kitą Internetu grįstą formą komunikavimui, reikalaujančiam nebegauti ateityje komercinių elektroninio pašto pranešimų iš siuntėjo elektroninio pašto adresu, į kurį buvo siųstas pranešimas; (ii) atgalinis adresas ar Internetu paremtas mechanizmas gebėtų priimti tokius atsisakymo pranešimus ar komunikavimus ne daugiau nei 30 dienų po originalaus pranešimo gavimo.*“[27] Taigi JAV kodekso 7704 (a) (3) reikalauja, kad komerciniai elektroninio pašto pranešimai turėtų atgalinio elektroninio pašto adreso funkciją ar kitą internetu pagristą mechanizmą, kuris leistų gavėjui pateikti prašymą daugiau nebesiųsti komercinių elektroninio pašto pranešimų. Be to, aktas apibrėžia, kad komercinių pranešimų iniciatorius laikytųsi reikalavimo, suteikiančio galimybę atsisakyti pranešimo, pateikdamas gavėjui sąrašą ar meniu, iš kurio gavėjas galėtų pasirinkti atskirus

[27] Federal Trade Commission. Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress. 2005. P. 64-65 // http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf; prisijungimo laikas: 2008-02-25.

pranešimų tipus, kurių gavėjas nenori gauti. Tačiau gavėjui, pranešime pateikus tokį sąrašą, turėtų būti sudaroma galimybė ateityje atsisakyti ne tik tam tikrų tipų, bet ir apskritai visų pranešimų. Taigi, kaip matyti, skirtingai nei Lietuvoje, Australijos ir JAV *anti-spam* aktuose labai panašiai formuluojamos nuostatos dėl elektroninių komercinių pranešimų, kuriems yra privalomas atsisakymo funkcijos įgyvendinimo mechanizmas. Abiejų valstybių *anti-spam* aktuose yra aiškiai pateikiama, kaip elektroninio pašto savininkai gali išreikšti savo valią, norėdami atsisakyti elektroninių komercinių pranešimų. JAV akto 5(a)(3)(C) skyriuje pateikiamas ir savotiškas saugus „prieglobstis“ siuntėjams, kai tam tikrais nenumatytais atvejais atgaliniai adresai ar kiti mechanizmai dėl techninių problemų be siuntėjo žinios neveikia nenumatytą laiko tarpą, tai tuo laikotarpiu siuntėjas turi teisę nepatenkinti gavėjo reikalavimų. Tačiau pašalinus techninius gedimus, komercinių elektroninio pašto pranešimų siuntėjas nedelsdamas turi įvykdyti prievolę.

Analizuojant Argentinos ir Rusijos galiojančius teisės aktus, pastebėta, kad nustatytų konkrečių reikalavimų elektroniniams komerciniams pranešimams, nagrinėjant atsisakymo funkcijos įgyvendinimo mechanizmus ir tikslių siuntėjo duomenų įtraukimą į elektroninius komercinius pranešimus, apskritai nėra.

Atsisakymo funkcija yra pakankamai svarbi, nes jos tikslas yra užtikrinti, kad gavėjas turėtų veiksmingą priemonę savo pasirinkimui įgyvendinti ir negautų ateityje komercinių elektroninių pranešimų iš konkretaus siuntėjo. Vis dėlto, kai kurie elektroninio pašto savininkai skeptiškai žiūri į *opt-out* mechanizmų naudojimą, nes pasitaiko atvejų, kuomet gavus komercinį elektroninio pašto pranešimą ir pasinaudojus teisės akte nurodytu atsisakymo funkcijos įgyvendinimo mechanizmu, *spameriams* yra duodamas signalas, kad jie rado „gyvą“ adresą. To pasėkmė gali būti elektroninio pašto dėžutės užkimšimas *spam* ar net blogiau – kenkėjišku *spam*.

Kadangi dažniausiai elektroniniai komerciniai pranešimai yra siunčiami reklamos tikslais, todėl kitas gana svarbus elektroninio komercinio pranešimo sudėtinis elementas – informavimas, kad pranešimo turinys yra reklaminio pobūdžio. „Reklama yra visiškai ar bent jau iš dalies subjektyviai pateikiama informacija, todėl turi būti aiškiai atskiriama nuo bet kokios kitos informacijos, t.y. vartotojas turi suprasti ar bent jau turėti galimybę suprasti, kad pateikiama informacija yra reklama, kaip subjektyvi informacijos forma, pateikiama kartu su bendrojo pobūdžio informacija, kuri pagal turinį paprastai yra objektyvi ir kurią skleidžiant nesiekiama tam tikro tik reklamai būdingo tikslo (skatinti vartotojus įsigyti prekių ar paslaugų), dėl tokios informacijų samplaikos vartotojai gali nesusigaudyti ir gali būti suklaidinti dėl tikrojo informacijos pateikimo tikslo. Todėl reklama turi būti aiškiai atskiriama (vaizdo garso

priemonėmis ar kitais būdais) nuo bet kokios kitos bendro pobūdžio informacijos“[28]. Nors reklamos atpažįstamumo principas, įtvirtintas LR reklamos įstatymo 3 straipsnyje, yra Lietuvoje taikomas daugiau tradicinei reklamai, jis yra labai svarbus ir elektroninėje erdvėje. Aiškinant šią reklamos įstatymo nuostatą, būtų galima teigti, kad minėtam reklamos atpažinimui elektroniniame pašte yra skirtas pranešimo **laukelis „tema“ (angl. *subject*) arba antraštė.** Vartotojas, atsidaręs elektroninio pašto dėžutę, iš anksto, t.y. net neatidaręs pranešimo, būtų informuojamas, kad gauto pranešimo turinys yra reklaminio pobūdžio. Tai itin aktualu didelių kompanijų darbuotojams, kasdien gaunantiems šimtus elektroninių laiškų, ir elektroninio pašto savininkams iš šalių, kuriose yra laikomasi *opt-out* metodo. Nors tokia konkreti nuostata dėl reklamos atpažinimo elektroninėj erdvėje nėra įtvirtinta nei reklamos įstatyme, nei kitame teisės akte, vis dėlto ES Elektroninės komercijos direktyva numato ES valstybėms narėms komercinių pranešimų sąlygas, kurių viena – kad *„būtų galima aiškiai nustatyti, kad tai yra komercinis pranešimas.“* [29] Tai yra reklamos principinė nuostata, kurios turėtų būti paisoma nepriklausomai nuo reklamos išraiškos priemonių – ar tai būtų televizija, radijas ar elektroninė erdvė. Vis dėlto, žvelgiant į šių dienų Lietuvos teisės aktus, reklama internete, nepaisant jos pateikimo ir naudojimo specifikos, reglamentuojama tik bendrosiomis reklamai taikomomis teisės aktų nuostatomis ir jokių specifinių nuostatų ar reikalavimų reklamai, pateikiamai internete, kol kas nėra.

Šiuo metu, kaip teigiama viename *Sophos* leidinių, „ypač populiarus tapo naudojimasis tam tikrais socialiniais interneto puslapiais, kaip *„Facebook“*, *„My Space“*, *„Bebo“* ir kt., kurie netrukus tapo kompiuterinių nusikaltimų priemonėmis. Dalis vartotojų jau perprato *spam* antpuolius elektroniniame pašte, tačiau yra mažiau atidūs kitais „keliais“ gaunamiems pranešimams - pvz., per *„Facebook“* ar kitą greitąjį susirašinėjimą žinutėmis.“[30] Lietuvoje galėtų būti tarp jaunimo paplitęs interaktyvus puslapis *„One“*, *„Frype“*. *Spameriai*, naudodamiesi šia vartotojų socialine priklausomybe, apsimeta esą tos socialinės internetinės bendruomenės nariais ir atsiunčia „draugišką“ pranešimą, kuriame pateikia nuorodą į tam tikrą internetinį puslapį ir „rekomenduoja“ pirkti nurodytame puslapyje tam tikras prekes, pvz., lieknanantį poveikį turinčius preparatus moterims ar ypač populiarų preparatą vyrams - *„viagra“*. (Priedas Nr. 3, *spam* per *Facebook* iš *„Sophos“* (anglų kalba).

[28] L. Markauskas. Reklamos teisinis reglamentavimas: teorija ir praktika. – Vilnius: UAB „Mokesčių srautas“, 2008. P. 26.

[29] Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1.

[30] Sophos security threat report update 07/2008. Social/business networking spam and malware. P. 11 // www.sophos.com/news/2008/07/dirtydozjul08.html; prisijungimo laikas: 2008-10-10.

Be to, svarbu, kad pateikiama reklama būtų ne tik atpažįstama, tačiau ir teisinga, kas dažnai yra nebūdinga, ypač kalbant apie kenkėjiško pobūdžio pranešimus. Pavyzdžiui, 2008 metų 3 ketvirtį, lyginant su 2007 m. tuo pačiu ketvirčiu, IT apsaugos ir kontrolės firmos „*Sophos“* duomenimis buvo 8 kartus daugiau kenkėjiškų priedų (angl. *atachments*), platinamų su elektroniniais pranešimais. Prie 1 iš 416 pranešimų liepos – rugsėjo mėnesiais buvo prikabintas pavojingas priedas, sukurtas užkrėsti pranešimo gavėjo kompiuterį. „Sophos“ identifikavo, kad dauguma užkrėstų priedų yra plataus masto kenkėjiškų atakų, kurias sukuria *spameriai*, pasekmė. Viena iš daugiausiai žalos padariusių atakų buvo *Agent HNY Trojan* virusas, kuris buvo užmaskuotas ir platinamas Pingvino *Panic apple iPhone* populiaraus žaidimo pavidalu. Operacinės sistemos „*Windows*“ vartotojai, atidarydami tokį gauto pranešimo priedą, sukelia pavojų savo kompiuteriuose esantiems asmens duomenims bei finansams.

JAV teisės akto 5 dalyje yra aiškiai nurodyti reikalavimai siunčiamiems pranešimams: (1) *kiekvienam žmogui yra draudžiama siųsti į apsaugotą kompiuterį komercinio elektroninio pašto pranešimus, susidedančius iš informacijos, kuri yra iš esmės neteisinga ar klaidinanti... (2)draudžiama siųsti pranešimus, nurodant neteisingą pranešimo temos antraštę* (angl. *subject*)*“*

15 U.S.C. 7704 (a)(2) draudžia komercinius elektroninio pašto pranešimus, kurie turi klaidinančią ar apgaulingą antraštę (angl. *subject line*). Antraštės nepateikimas gali užtraukti siuntėjui atsakomybę. Vis dėlto, kaip teigia FPK, ši priemonė yra naudinga vartotojams, nes jie gali iš anksto sužinoti pranešimo pobūdį, o *spameriams* tai yra nemaža kliūtis platinti *spam.* Ši sąlyga yra viena iš priemonių, drausminančių *spamerius*: jie gali nurodyti teisingai įvardytas antraštes ir rizikuoti, kad jų pranešimas nebus perskaitytas ar naudoti apgaulingas temos formuluotes ir rizikuoti, jog bus patraukti baudžiamojon atsakomybėn. Federalinė prekybos komisija, 2005 m. tirdama su *spam* susijusias bylas, aštuoniose bylose iš 20 patvirtino pažeidimus, susijusius su apgaulingos antraštės pateikimu. Komisija nustatė tokius teisės pažeidimus:

a) siuntėjas neteisingai nurodo, kad turėjo ankstesnius ryšius su gavėju;

b) apgaulinga antraštė informuoja, kad pranešimą su aktualia tema atsiuntė IPT;

c) klaidinanti antraštė, kuri buvo visai nesusijusi su turiniu.

15 U.S.C. 7704 (a)(5)(A)(i) įpareigoja, kad *kiekvienas komercinis elektroninio pašto pranešimas turėtų aiškius ir išsiskiriančius reklamos ar prekybos* (angl. *solicitation*) ženklus, net jei ir buvo duotas išankstinis sutikimas. Šio reikalavimo tikslas yra pateikti pastabą, kad į elektroninio pašto dėžutę gautas pranešimas yra reklama, kuri signalizuotų gavėjams, kad pranešimas yra komercinio pobūdžio, ir nulemtų greitą jų apsisprendimą – ištrinti arba perskaityti pranešimą.

FPK nagrinėdama *spam* bylas, 3-ose iš 20 nustatė minėtą pažeidimą. Vienoje iš bylų, kaltinamojo siųstame elektroniniame pranešime klaidingai traktuojama, kad gavėjas teiravosi apie nekilnojamojo turto paslaugas ir turėjo ankstesnį ryšį su kaltinamuoju, todėl ir nenurodė aiškių ir išsiskiriančių reklamos ar prekybos ženklų. Kitoje byloje Komisija kaltino siuntėją dėl išsiųstuose elektroninio pašto pranešimuose pateiktos klaidingos informacijos vartotojams. Jiems būdavo nurodoma, kad jų kompiuteriai esą nuskanuoti ir juose rasta šnipinėjimo programa „*spyware*“. Apgaulinga informacija nukreipė vartotoją į internetinį puslapį neva nemokamai įsigyti programinės įrangos, kuri padėtų išspręsti iškilusią problemą. Trečioji byla, kurioje pranešimo siuntėjas buvo kaltinamas pažeidęs teisės normas, nes platindamas apgaulingą dietinių papildų išpardavimą nepateikė reklamos nuorodos.

Reikalavimas identifikuoti reklamą gana veiksmingai padeda FPK ir kitiems įgaliotiems atstovams traukti *spamerius* baudžiamojon atsakomybėn. Vis dėlto įrodyti, kad trūksta reikalaujamos reklamos identifikacijos, yra santykinai lengviau negu įrodyti, jog elektroniniame pranešime informacija yra klaidinga ar apgaulinga.

Dar viena išskirtinė JAV *Can spam* akte įtvirtinta nuostata dėl prievolės įdėti įspėjamuosius ženklus apie seksualinio-intymaus pobūdžio komercinius elektroninius pranešimus. Specifiniai komerciniai elektroniniai pranešimai, kurie susideda iš seksualiai orientuotos medžiagos, privalo turėti tam tikrus ženklus ar pastabas pranešimo antraštėje (angl. *subject line*), kurie įspėtų gavėją apie pranešimo turinį. Neleistina pranešimo pradžioje, matomoje vietoje, įdėti seksualiai orientuotą vaizdinę medžiagą. Reikalaujama pateikti atitinkamus sutartinius ženklus ar pastabas apie seksualinio pobūdžio turinį, nurodant siuntėjo galiojantį fizinį pašto adresą, pranešimo atsisakymo mechanizmą ir instrukcijas, kaip prisijungti prie atitinkamą turinį pateikiančio internetinio puslapio.

Sutinkamai su 15 U.S.C. 7704 (d)(3) nuostatomis, Komisija promulgavo taisyklę, kuri nurodo frazę „seksualiai atvira“ (angl. SEXUALLY-EXPLICIT) įtraukti į kiekvieno pranešimo antraštę ir ją dar kartą pakartoti pranešimo turinio pradžioje. Ši suaugusiems vartotojams taikoma taisyklė (angl. „Adult Labeling Rule“ („ALR“)) įsigaliojo 2004 m. gegužės 19 dieną.

Can spam ir ALR suteikia vartotojams dvi naudingas apsaugas nuo nepageidaujamų pornografinių elektroninių pranešimų. Pirmoji, reikalavimas antraštėje pažymėti signalus gavėjams, kad elektroninis pranešimas turi seksualiai atviros medžiagos ir palengvina gavėjams pasirinkti ar atsisakyti tokio tipo pranešimų. Antra, jei vartotojas netyčia ir atidarytų tokį pranešimą, jis būtų apsaugotas nuo seksualiai orientuotos medžiagos poveikio. Šios nuostatos esmė yra ta, kad tokiu būdu yra bandoma apsaugoti vaikus nuo lengvo priėjimo prie pornografinio turinio *spam*.

Deja, kalbant apie **Argentinoje** galiojančius teisės aktus, reikia pripažinti, kad juose nėra numatytų jokių panašaus pobūdžio sąlygų, kurios būtų keliamos elektroniniams komerciniams pranešimams. Būtų galima paminėti kai kurias įdomias Argentinos 2004 m. ***Anti-spam* įstatymo projekto,** kuris kongreso buvo atmestas greičiausiai dėl per griežtų kai kurių teisės normų, **nuostatas**. Įstatymo projekte numatyta, kad siuntėjas privalo:

a)pranešimus siųsti iš elektroninio pašto adreso, kuris susidėtų iš šioje įstatymo nuostatoje pateikto pavyzdžio elementų: ADV-CUIT@dominio; i) „ADV“ turi būti pateikiamas be jokių tarpų, didžiosiomis raidėmis, be kitų skyrybos ženklų. „ADV“ reiškia, kad kalba eina apie elektroninio pašto komercinį pranešimą. ii) „-„neilgas ženklas, pateikiamas ne apačioj, o kaip „minus“ ženklas. iii) CUIT –unikalus siuntėjo identifikavimo raktas, be tarpeli, be kitų skyrybos ženklų. iV) domeno vardas, galiojantis ir atitinkantis numatytus įstatymų domeno reikalavimus.

b) susilaikyti nuo elektroninių pranešimų siuntimo iš elektroninio pašto sąskaitos;

c) pasirašyti elektroninio pašto komercinį pranešimą;

d) prie siunčiamo komercinio elektroninio pašto pranešimo pridėti elektroninį sertifikatą, kuris patvirtintų siuntėjo elektroninio pašto adreso tikrumą ir suteiktų teisę reklamuoti tam tikras prekes ar paslaugas elektroninio pašto pagalba. Šį sertifikatą suteikia sertifikuojanti įstaiga;

e) įtraukti į pranešimo temos (angl.„subject“) laukelį reklamą simbolizuojantį raidžių junginį – „ADV“;

f) į pranešimo turinį įtraukti siuntėjo identifikacinius duomenis;

h) pranešimo pabaigoje įtraukti tekstą: „šitas pranešimas atitinka elektroninio pašto komercinių pranešimų siuntimo įstatyme numatytus reikalavimus“;

i) į pranešimo turinį įtraukti informaciją, kad gavėjas gali įtraukti savo elektroninio pašto adresą į atsisakymo registrą (isp. Registro Nacional De opt-out), kuris įgyvendinamas šituo įstatymu;

j) į pranešimo turinį įtraukti informaciją, kad gavėjas, gavęs komercinį elektroninio pašto pranešimą, bet kuriuo momentu gali atsisakyti gauti ateityje tokius pranešimus, kuriuos siunčia siuntėjas. Į pranešimą yra privaloma įtraukti galiojantį atgalinį elektroninio pašto adresą, į kurį gavėjas gali nusiųsti elektroninio pašto pranešimą, kuriuo praneštų apie savo valią ar apsisprendimą nebegauti naujų elektroninio pašto komercinių pranešimų iš konkretaus siuntėjo. Be visų šitų elektroniniam komerciniam pranešimui keliamų sąlygų, projekto kūrėjai numatė, kada siuntėjas, kuris neturėjo išankstinio komercinio ir asmeninio ryšio su gavėju, privalo laikytis minėtų reikalavimų, nesiųsti pranešimų adresais, kurie įtraukti į atsisakymo registrą. Taip pat projekto kūrėjai nusprendė nustatyti tam tikrą elektroninio pranešimo dydį

(kilobaitais), kurio neturėtų viršyti siunčiami pranešimai. Rengiant įstatymo projektą greičiausiai nebuvo galutinai apsispręsta dėl elektroninio pašto komercinio pranešimo dydžio, todėl konkretus kilobaitų skaičius nebuvo įvardytas.

Kaip matyti, jei šis projektas būtų promulguotas, jis gana stipriai varžytų legalių elektroninių komercinių pranešimų siuntėjų veiksmus. Siuntėjams reikėtų gauti tam tikrus sertifikatus, laikytis nustatytų pranešimų dydžio. O tokia nuostata, kaip „susilaikyti nuo elektroninių pranešimų siuntimo iš elektroninio pašto sąskaitos“ būtų galima teigti, kad prieštarauja reklamos ir elektroninio pašto esminiams principams. Reklama yra skirta platinti, skleisti informaciją, siekiant asmenis supažindinti su įvairių produktų, paslaugų, prekių egzistavimu. Todėl suprantama, kad kai kurios nuostatos yra sunkiai įgyvendinamos ir ne visai logiškos. Beje, Argentinos Kongreso netenkino šis įstatymo projektas, kad taptų įstatymu, todėl buvo atmestas. Argentinos elektroninio pašto savininkams dar kurį laiką teks ginti savo teises remiantis asmens duomenų apsaugos įstatymo nuostatomis.

Rusijoje galiojantys įstatymai, kaip ir Lietuvoje bei Argentinoje, labai išsamaus ir konkretaus reglamentavimo nepateiks nagrinėjamais aspektais. Būtų galima paminėti įstatymą „Dėl teisėto interneto paslaugų perdavimo reguliavimo“ (angl. *Bill ‘On Legal Regulation of Rendering Internet Services‘*), kurio 33 straipsnyje siuntėjui, siunčiančiam reklaminius pranešimus, keliamas reikalavimas šių pranešimų laukelyje „tema“ (angl. „subject“) įrašyti frazę „remiantis reklamos teisėmis“ *(angl. „on the rights of advertising“*). Tai vienintelė rasta Rusijos teisės numatyta sąlyga dėl elektroninių komercinių pranešimų.

Australijos *Spam-act* gana išsamiai reglamentuoja elektroninių komercinių pranešimų siuntimo sąlygas ir kai kurių elektroninio komercinio pranešimo sudėtinių elementų įtraukimo prievoles, tačiau reklamos atpažinimo požymių ar informacijos pateikimo antraštėje apie pranešimo turinį šis įstatymas nereglamentuoja.

Vis tik Australijos įstatymas, priešingai nei visų kitų nagrinėjamų valstybių teisės aktai, numato kitą įdomų bei originalų reikalavimą, kuris yra ypač aktualus ir susijęs su paskutiniu metu plintančiomis *spam* formomis. Australijos *Spam akto* 16 straipsnyje nurodo, jog „*Draudžiama siųsti pranešimą* ***neegzistuojančiais elektroniniais adresais.***

Asmenims draudžiama siųsti ar liepti siųsti komercinius elektroninius pranešimus neegzistuojančiais elektroniniais adresais: jei asmuo neturėjo priežasties manyti, kad elektroninis adresas egzistuoja; ir jei elektroninis pranešimas turi australišką nuorodą ir nėra paskirtasis komercinis elektroninis pranešimas. Ši nuostata negalioja, jei asmuo (siuntėjas) nežinojo ar negalėjo ir norėdamas sužinoti, kad pranešimas turi Australijos nuorodą. Tačiau jei siuntėjas nori remtis šia nuostata, jam tenka prievolė įrodyti nežinojimo faktą.“

Susipažinus su šia teisės norma, galbūt ne vienam, mažiau žinančiam apie *spam* suktybes, iškiltų abejonė dėl tokios normos būtinybės įtraukti ją į įstatymą. Australijos įstatymų leidėjas greičiausiai numatė tokias galimas *spamerių* gudrybes kaip „žodynų atakos“, kuomet yra pasitelkiamos tam tikros programos, sudarinėjančios pagal žodžius iš žodynų, pagal tam tikrus vardus ir skaičius galimus, bet nebūtinai realiai egzistuojančius, elektroninių pranešimų adresus. Vis dėlto atsirado ir dar viena *spamerių* gudrybė, susijusi su *spam* siuntimu neegzistuojančiais adresais. Kaip teigiama „*Sophos“* pranešime, „per 2008 m. pirmąjį pusmetį pastebima *spam* banga išaugusiu nepristatytų ir grįžusių atgal laiškų pranešimų (angl. *non-deliveryreport*) skaičiumi. Tokie pranešimai yra kuriami elektroninio pašto sistemų, kurie priima *spam* pranešimus SMTP[31] sesijos metu. Jei yra tam tikras pristatymo gedimas (tai akimirkai, pašto dėžutė yra pilna ar vartotojas neegzistuoja), sistema bando grąžinti nepavykusį pristatyti pranešimą atgal numatytam šio pranešimo siuntėjui.

Nepristatytas pranešimas yra nukreipiamas elektroninio pašto adresu, kurį sistema randa šio pranešimo siuntėjo informacijos vokelyje (angl. *the Return-Path header*). Kadangi šis adresas *spam* pranešimuose dažniausiai būna suklastotas, nepristatytas pranešimas nusiunčiamas į netikro siuntėjo elektroninio pašto dėžutę, iš kurios *spam* nebuvo išsiųstas.“ Šis *spam* platinimo būdas yra vadinamas „*backscatter spam*“ (liet. *atgal grįžtančio spam*). Specifiniai gavėjų adresai ar domenai, kurie yra populiarūs tarp *spamerių*, kasdien gali būti atakuojami šimtais ar net tūkstančiais tokio pobūdžio „*backscatter spam“*.

JAV ir Australijos *anti-spam* teisės aktai numato ir kitas specifines prievoles susilaikyti nuo tam tikrų veiksmų, kurie kitų nagrinėjamų valstybių įstatymuose nėra numatyti. Kaip didinančius atsakomybę pažeidimus (angl. *aggravated violations*) minėtų abiejų valstybių teisės aktai numato dažnai *spamerių* naudojamas priemones, leidžiančias *spameriams* padidinti siunčiamų pranešimų mastą: kompiuterinius įsilaužimus, adresus renkančias (angl. *address „harvesting*“) programas, „žodynų atakas“ (angl. *„dictionary attacks*“), kompiuterines programas, automatiškai kuriančias elektroninio pašto dėžutes.

JAV„(A) yra laikoma neteisėta :

(i)naudoti interneto puslapius, kai gavėjų elektroninio pašto adresai išgaunami naudojant automatines priemones [...]

(ii) gavėjų elektroninio pašto adresai išgaunami automatiniais būdais, t.y. sudarinėjant galimas elektroninio pašto adresų kombinacijas iš vardų, raidžių bei skaičių ar jų derinių.“

[31] SMTP „(angl. *Simple Mail Transfer Protocol*) – paprastas pašto perdavimo protokolas – *de facto* standartas el. pašto laiškų perdavimui internete. Naudojamas elektroniniams laiškams pristatyti į gavėjo el. pašto dėžutę [...] Siunčiančioji pusė (klientas) duoda tekstines komandas, gaunančioji (serveris) apie komandų vykdymo rezultatus praneša grąžindama klaidų (būsenos) kodus“. Pasinaudota informacija iš http://lt.wikipedia.org/wiki/SMTP; prisijungimo laikas:2008-11-27.

Can-spam aktas draudžia gavėjų adresus sudarinėti naudojantis žodynais. Daugybė *spamerių* naudoja automatines programas, kurios automatiškai ieško ir renka elektroninio pašto adresus iš įvairių internetinių tinklalapių, svetainių, adresų sąrašų ir kitų internetinių išteklių. Tokiu būdu surinktus adresus galima naudoti *spam* siuntimui.

Yra draudžiama: (2*) naudoti tam tikras automatizuotas priemones, kurių pagalba galima prisiregistruoti prie daugybės elektroninio pašto dėžučių.*

(3) persiųsti naudojantis kito siuntėjo atgaliniu adresu komercinius elektroninio pašto pranešimu [...]be autorizavimosi.

Can-spam aktas laiko neteisėtu veiksmu automatizuotų techninių priemonių (programų) naudojimą, kurių pagalba prisiregistruojama prie kitų asmenų elektroninio pašto dėžučių su tikslu išsiųsti masinius nepageidaujamus komercinius elektroninius pranešimus.

Panašiai kaip ir JAV, Australijos *Spam act* 3 dalyje yra numatyta, kad Australijoje gyvenantiems asmenims ar Australijoje veiklą vykdančioms organizacijoms draudžiama ne tik naudoti programinę įrangą (angl. *address – harvesting software*), kuri ieško internete galimų elektroninio pašto adresų ir juos apdoroja, bet ir ją platinti bei įsigyti. Taip pat nurodoma, kad draudžiama parduoti, įsigyti ir apskritai naudoti tokia programine įranga surinktus elektroninių pašto adresų sąrašus (angl. *harvested – address lists*).

Išanalizavus šiuose skirsniuose su elektroniniais komerciniai pranešimais susijusias įvairių teisės aktų nuostatas, pastebima, kad susiduria ir persipina kelios teisės šakos: asmens duomenų apsaugos, reklamos, vartotojų apsaugos ir informatikos (interneto) teisė. Todėl nekelia nuostabos, kad elektroninių komercinių pranešimų siuntėjams turėtų būti pakankamai sunku „išlaviruoti“, nepažeidžiant kurio nors iš teisės aktų. Esant tokiam plačiam teisių ir pareigų spektrui, eiliniam vartotojui gali būti sunku suvokti, kuriuo įstatymu remtis ir į kurią instituciją kreiptis, norint ginti savo teises. Gerai, jei su *spam* susijusios normos yra susistemintos į vieną teisės aktą, tačiau, kaip matyti, nemaža dalis valstybių *spam* atžvilgiu neturi vieningo teisės akto. Atskirų valstybių gyventojams, besinaudojantiems viena globalia interneto erdve, problema tampa ne tik atskirų valstybių teisės aktų įvairovė, bet ir juose įtvirtintų skirtingų reikalavimų (pareigų) įvairovė, už kurių nesilaikymą yra taikomos valstybės prievartos priemonės – sankcijos. O teisėje įtvirtinta nežinojimo prezumpcija teigia, kad įstatymų nežinojimas – neatleidžia nuo atsakomybės.

2.3. Jurisdikcijos ir *spam* siuntėjui taikomos atsakomybės problematika

„Teisinė atsakomybė – tai pareiga atsakyti už padarytą blogį,
ji atsiranda kaltai padarius skriaudą ar blogį,
pasireiškiantį neatlikimu to, ką žmogus privalėjo atlikti“
H.Grocijus

Nagrinėjant *spam* kaip teisei prieštaringą reiškinį, būtina kalbėti apie *spam* siuntėjo atsakomybę ir apie valstybės numatytas sankcijas, be kurių praktiškai atsakomybė neįmanoma. „Sankcija yra priemonė, leidžianti žemesniu lygiu grąžinti teisės pažeidėjo teisiniam statusui teisių ir pareigų pusiausvyrą, kuri buvo pažeista teisių naudai atitinkamos pareigos nevykdymu. Sankcija yra ir teisių ribojimo mastelis, nurodantis, kokia teisės pažeidėjo teisė ribojama, likviduojama ir kokia apimtimi.“[32]

Atkreiptinas dėmesys, kad *spameriams* už *spam* siuntimą ar už elektroniniams komerciniams pranešimams keliamų turinio reikalavimų pažeidimus atskirose valstybėse yra numatytos ne tik skirtingos sankcijos, bet ir skirtingos atsakomybės rūšys. Pavyzdžiui, už padarytą pakartotinį pažeidimą į elektroninio pašto dėžutę, siunčiant *spam*, Lietuvos įstatymuose numatyta administracinė atsakomybė - maksimali bauda 2000 Lt. Australijos Federalinis Teismas, remdamasis civilinių nuobaudų nuostatais (angl. *civil penalty provision*), už tokį pažeidimą gali priimti sprendimą ir paskirti asmeniui sumokėti Britanijos tautų sandraugai (angl. *the Commonwealth*) baudą net iki 10 000 baudos vienetų (angl. *penalty units*)[33]. Argentinos teismai, pagal 2003 m. Asmens duomenų apsaugos įstatymo 31 skirsnio nuostatas tokio pobūdžio pažeidimą pripažinę labai rimtu[34] pažeidimu, galėtų skirti net iki 100 000 pesų[35] baudą. JAV tokį pažeidimą gali pripažinti net nusikaltimu ir skirti ne tik piniginę baudą žalai atlyginti, tačiau ir nuteisti laisvės atėmimu iki 5 metų ar net daugiau. Pagal Rusijos Federacijoje galiojantį Administracinį kodeksą maksimali bauda gali būti 1850 JAV dolerių, tačiau teismų praktikoje pasitaikė precedentas, kuomet *spameris* buvo nuteistas 1 metus kalėjimo.

Taigi, kaip matyti, yra taikomos įvairios priemonės, kuriomis siekiama atstatyti išbalansuotą teisių ir pareigų pusiausvyrą. Tačiau šis pavyzdys akivaizdžiai atskleidžia, kad už

---

[32] A. Vaišvila. Teisės teorija. - Vilnius: Justitia, 2004. P. 446-447.
[33] pagal Australijoje galiojantį teisės akto „Crimes Act 1914“ 4AA punktą 1 baudos vienetas lygus 110 Australijos dolerių // http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s4aa.html; prisijungimo laikas 2008-10-02.
[34] Vadovaudamasi Argentinos asmens duomenų apsaugos įstatymo 31 straipsnio nuostata 2003 m. Argentinos duomenų apsaugos agentūra priėmė dispoziciją (Disposition N°. 1/2003), pagal kurią Asmens duomenų apsaugos įstatymo pažeidimai klasifikuojami į smulkius (angl. m*inor*), rimtus (angl. *seriuos*) ir labai rimtus (angl. *very seriuos*) // http://www.protecciondedatos.com.ar/law12003.htm; prisijungimo laikas: 2008-10-15.
[35] 2008-11-27 1 JAV doleris lygus 3,32270 Argentinos pesų // http://www.xe.com/ucc/convert.cgi; prisijungimo laikas: 2007-11-27.

spam platinimą atskirose valstybėse gali būti taikomos ne tik skirtingos sankcijos, bet ir teisinės deliktinės atsakomybės rūšys. Prisiminus teisės esmę - teisių ir pareigų vienovę - kyla klausimas, kodėl Internete – vienoje globalioje erdvėje – padarius tokio paties pobūdžio teisės pažeidimą, t.y. kuomet teisių turėtojas atsisako vykdyti tokio paties pobūdžio pareigą, kurios vykdymą įstatymai laiko būtinu siekiant legalizuoti to asmens teises visuomenėje, teismams vykdant teisingumą teisių ir pareigų pusiausvyra atstatoma ribojant skirtingo lygio to asmens subjektines teises. Kalbant apie skirtingas sankcijas, pvz., skiriant skirtingo dydžio pinigines baudas, galbūt būtų galima iš dalies pateisinti atsižvelgus į skirtingą valstybių ekonominį išsivystymą ir pragyvenimo lygį, tačiau, kaip matyti, tam tikrais atvejais gali būti taikoma ir viena iš baudžiamosios teisės prievartos priemonių – laisvės (vienos asmens prigimtinių teisių) ribojimas.

Reikėtų nepamiršti, kad kai kuriose užsienio valstybėse baudžiamoji teisė dažnai suprantama kiek kitaip – plačiau negu, pvz., Lietuvoje. Ji apima ir tas veikas, kurios pas mus turi administracinių teisės pažeidimų statusą, t.y. baudžiamoji teisė apima ir tas veikas, kurios yra baudžiamos. Tai būtų, pavyzdžiui, ir tokios veikos kaip įvairūs eismo saugumo taisyklių pažeidimai. Čia nusikaltimas yra ir tai, kas yra nusikaltimas tradicine prasme, ir tai, kas yra kitoks teisės pažeidimas (nusižengimas). Dėl tos priežasties skiriasi atskirų valstybių pažeidimų ir nusikaltimų statistika. JAV baudžiamoji teisė suprantama dar plačiau. Čia „*Criminal law*“, be administracinės ir baudžiamosios teisės, apima ir baudžiamąjį procesą. Baudžiamasis procesas JAV yra neatsiejamas nuo baudžiamosios teisės.

Tačiau būtų galima teigti, kad nepriklausomai nuo to, kokia teisės šaka reguliuoja teisinius santykius, vis dėlto už santykius reguliuojančių teisės normų pažeidimą turėtų būti taikomos vienodos teisinės atsakomybės sankcijos.

Kalbant apie baudžiamosios atsakomybės taikymą, verta pažvelgti giliau į konkrečius teisės aktus, o ypač į galiojančius JAV, ir panagrinėti, kokios su *spam* susijusios veikos yra kriminalizuojamos. Atsakomybė už *Can spam* akto įgyvendinimą ir baudžiamųjų priemonių taikymą tenka Teisingumo Departamentui (*Department of Justice*). *18 U.S.C.* 1037 (a) punktas kriminalizuoja veiklas (angl. *activities*), kurias *spameriai* vykdo, kad išvengtų IPT naudojamų *anti-spam* filtrų ir išsisuktų nuo atsakomybės dėl veiklos, susijusios su *spam*. Išskiriamos penkios veiklos:

1. prisijungimas prie neapsaugoto kompiuterio be autorizavimosi, kad išsiųstų masinį *spam*.

2. naudojimas atvirų tinklų (angl. *Open relays*) su tikslu apgauti siunčiant masinį komercinį *spam*. (Ši nuostata buvo suformuota siekiant apsaugoti vartotojus nuo *spamerių*, kurie naudoja atvirus tinklus ar atvirus *proxy* serverius, kad nuslėptų savo identifikaciją.)

3. Klaidingų antraščių naudojimas.

4. Apgaulingas elektroninio pašto dėžučių ar domenų vardų kūrimas, kurie būtų naudojami siųsti masinius komercinius elektroninius pranešimus.

5. Apgaulingas tvirtinimas esant užsiregistravus Interneto protokolo (IP) adresu *spam* siuntimui.

Pastaroji nuostata kriminalizuoja *spamerių* naudojamas apgaulingas technikas, kad išgautų IP adresus, neįtrauktus į juoduosius sąrašus. *Spameriai* naudoja neegzistuojančioms kompanijoms ar registruotiems asmenims priklausančius registruotus IP adresus, kad apgaudami IPT įgyvendintų savo tikslus.

18 U.S.C.§ 1037 (b) įtvirtina maksimalias bausmes už 1037 skyriaus pažeidimus. Yra išskiriamos trys bausmių pakopos:

1**.** arba *bauda, arba laisvės atėmimas iki 5 metų, arba abu, jei - (B) kaltinamasis jau anksčiau buvo baustas už šiame straipsnyje nurodytas nusikalstamas veikas ar pagal bet kurios valstijos įstatymus baustas už elgesį, kuris apima masinių komercinių elektroninių pašto pranešimų siuntimą ar neautorizuotą (be leidimo) prisijungimą prie kompiuterių sistemos.*

2. *trijų metų maksimali laisvės atėmimo bausmė taikoma dėl nusikaltimų arba pagal* 1037(a) (1) arba pažeidus 1037(a) (2) – (5) nuostatas, kai yra bent viena iš atskirų papildomų sąlygų. Sąlygos siejamos su finansiniu nuostoliu ar kita žala gavėjui, išsiųstų elektroninių laiškų apimtimi, neteisėtų registracijų mastu, ar jei kaltinamasis vadovavo darant nusikaltimą. Pvz., bauda pagal šį straipsnį ar įkalinimas ne daugiau kaip 3 metai arba abu, taikomi, jeigu

„- nusikaltimas padarytas pagal (4) punktą ir įtraukiant 20 ar daugiau suklastotų elektroninių pranešimų, ar 10 suklastotų domeno vardų registracijų;

- išsiųstų elektroninių pranešimų apimtis viršija 2500 per 24 valandas, 25000 per 30 dienų laikotarpį arba 250000 per metus;

- nusikaltimas vienam asmeniui padarė vienkartinę 5000 dolerių žalą arba tokio pat dydžio materialinę žalą per kelis kartus vienerių metų laikotarpiu“.

Kaip teigiama viename FPK 2005 m. gruodžio mėnesio pranešime Kongresui, tai viena dažniausiai JAV taikomų sankcijų ir daugiausiai suformuotų precedentų. Pvz., 2004 m. rugsėjo mėnesį Nicholas Tombros buvo pripažintas kaltu Kalifornijos Centrinėje apygardoje dėl 18 U.S.C. 1037 (a) (1) pažeidimo, kai *spam* siuntimui pasinaudojo bevielio namų interneto tinklais, kurie nebuvo deramai apsaugoti[36]. 2005 m. liepos mėnesį kita byla buvo nagrinėjama Džordžijos valstijos Šiaurės apygardoje, kur Peter Moshou taip pat pripažintas kaltu pažeidus minėtą straipsnį, kai prisipažino prisijungęs prie IPT kompiuterių be autorizavimosi, kad išsiųstų reklaminius pranešimus, susijusius su atostogų planavimo paslaugomis. „2005 m. lapkričio 17d.

[36] Žiūrėti www.usdoj.gov/usao/cac/pr2004/131.html Tombro nuosprendis buvo atidėtas.

Moshou buvo nuteistas 12 mėnesių laisvės atėmimo ir įpareigotas sumokėti 120 000 JAV dolerių restitucijos“[37].

3. Maksimali vienerių metų laisvės atėmimo bausmė gali būti skiriama dėl bet kurio nusikaltimo, numatyto skyriuje 1037. Šiuo atveju Teisingumo departamentas netaiko jokių sunkinančių ar lengvinančių aplinkybių.

Tačiau, kaip rodo paskutiniu metu plėtojama JAV teismų praktika, už padarytus nusikaltimus, susijusius su ***spam,*** asmeniui gali grėsti net ir 20 metų įkalinimo bausmė. 2007 m. JAV federalinis teismas suformavo vieną iš precedentų, susijusių su ***spam***. Robert Alan Soloway, žiniasklaidoje vadinamas ***spam*** karaliumi, siųsdavo milijonus nepageidaujamų komercinių elektroninio pašto pranešimų, naudodamasis sukompromituotų kompiuterių tinklais, kitaip dar vadinamais ***zombiais*** ar ***botnets***[38]. Pranešimų gavėjai, paspaudę ant atsiųstos nuorodos, esančios elektroniniame pranešime, būdavo nukreipiami į interneto puslapį, kuriame jis reklamuodavo dviejų tipų paslaugas. Viena iš paslaugų buvo pasiūlymas išsiųsti net iki 20 milijonų elektroninių komercinių pranešimų per 15 dienų už 495 dolerius. Kita paslauga, kai jis siūlė parduoti savo sukurtą programą, kurią įsigijęs pirkėjas galėtų išsiųsti elektroninius pranešimus 80-čiai milijonų adresatų. Jis apgaulingai tvirtindavo, kad elektroninio pašto adresai yra legalūs ir tie asmenys pageidauja gauti tokius pranešimus. Federalinis tyrimų biuras artimai bendradarbiaudamas su Teisingumo departamentu inicijavo operaciją „***Botroast***“, kurios metu atskleidė tris ***spam*** schemas, tarp jų ir ***spamerio*** Soloway sukurtą schemą. Soloway buvo suimtas 2007 m. gegužės 29 d., praėjus savaitei po federalinio teismo prisiekusiųjų priimto kaltinamojo akto dėl 35 nusikalstamų veikų. Spameris kaltinamas pašto sukčiavimu (angl. ***mail fraud***), telefoniniu sukčiavimu (angl. ***wire fraud***), elektroninio pašto sukčiavimu – ***spam*** (angl. ***e-mail fraud***), tapatybės vagystėmis (angl. ***Identity theft***) ir pinigų plovimu.[39] Valstybės kaltintojas siūlė skirti ***spameriui*** išimtinai 20 metų laisvės atėmimo bausmę. Tačiau 2008 m. liepos 22 d. Vašingtono Vakarų apygardoje buvo priimtas nuosprendis – 47 mėnesių laisvės atėmimo ir trejų metų priežiūra po išleidimo iš kalėjimo. Be to, nuteistasis turės atidirbti 200 valandų visuomenei naudingų darbų. Apygardos teisėja Marsha Pechman ateityje dar turėtų priimti sprendimus dėl aukoms padarytos žalos atlyginimo. Vis dėlto 2008 m. rugsėjo 22d. prokurorai apskundė šį nuosprendį ir prašė pakeisti skirtą bausmę sugriežtinti, t.y. iki 9 metų laisvės atėmimo.

Taigi, kaip matyti, be baudžiamosios atsakomybės, JAV yra taikoma ir civilinė atsakomybė, kuomet nukentėjusysis gali pareikšti privatų kaltinimą dėl patirtos žalos atlyginimo.

---

[37] Bill Montgomery, Guilty Plea a Win for Spam Act, Atlanta Journal-Constitution, July 1, 2005, at 4E.

[38] Botnet – tai žargonas, kuriuo įvardijami programinės įrangos robotų rinkiniai, kurie veikia autonomiškai ir automatiškai. Terminas dažnai asocijuojamas su piktybine programine įranga, bet gali būti suprantamas ir kaip kompiuterinis tinklas, naudojamas kompiuterinės programinės įrangos platinimui.

[39] Informacija iš Department of Justice FY 2007 Performance and accountability Report, P. 43. // www.usdoj.gov/ag/annualreports/pr2007/msg-ag.pdf ; prisijungimo laikas: 2008-11-12

Bausmė už numatytų reikalavimų pažeidimus yra skirtinga. Bet iš esmės leidžiama civilinio proceso tvarka išieškoti patirtus nuostolius. Pvz., Merilendo valstijos teisė leidžia net tik gavėjui bylinėtis dėl to, kad *spam* gavėjo vardas ar domenas buvo neteisėtai naudojamas elektroniniuose pranešimuose, bet ir trečiajai šaliai – IPT, kurio tinklai buvo naudojami *spam* siųsti. *Spam* gavėjas ir trečioji šalis gali reikalauti padengti patirtus nuostolius ar reikalauti įstatymu numatytos 5000 dolerių baudos išieškojimo iš *spamerio*.

Verta paminėti Rusijoje vienintelę pasitaikiusią baudžiamąją bylą, iškeltą prieš *spamerį*, kuri buvo užbaigta 2004 m. – *Ural GSM vs. Androsov*. *Spameris* Androsovas išsiuntė apie 15000 nelegalių SMS pranešimų, įsilauždamas į SMS siuntimo centrą, priklausantį Ural GSM Co., Ltd. Androsovas buvo nubaustas 100 JAV dolerių bauda ir 1 metų laisvės atėmimu, tačiau antroji nuosprendžio dalis buvo atidėta. Nuosprendis buvo priimtas remiantis Baudžiamojo kodekso 273 straipsniu dėl veikos, susijusios su *spam* kūrimu, naudojimu ar platinimu.

Kalbant apie Lietuvos Respublikoje galiojantį Baudžiamąjį kodeksą, jame su *spam* platinimu susijusių konkrečių teisės normų šiuo metu nėra priimta. Nebent būtų galima paminėti 198^1 straipsnį, kuriame įstatymas numato už neteisėtą prisijungimą prie informacinės sistemos iki 1 metų laisvės atėmimo bausmę, arba 198^2 straipsnį, kuriame įstatymas numato už įrenginių ar programinės įrangos platinimą, taip pat slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų, tiesiogiai skirtų daryti nusikalstamas veikas, gaminimą, gabenimą, pardavimą ar kitokį platinimą, arba įsigijimą ar laikymą net iki trijų metų laisvės atėmimo. Šias normas būtų galima įvairiai interpretuoti ir taikyti, pavyzdžiui, asmenims, kurie yra sukonstravę tam tikrus įrenginius ar programas ir juos naudoja ar net platina nusikaltimams daryti, pvz., masiniam *spam* siųsti. Vis dėlto kvalifikuojant veikas pagal šiuos straipsnius, veika (objektinis teisės pažeidimo požymis), kuria būtų padarytas teisės pažeidimas, siejama ne su *spam* siuntimu, o su įvairių įrenginių ar programų naudojimu, laikymu ar su neteisėta prieiga. Kol kas nėra teismų praktikos, kuri bent iš dalies sietų 198^2 straipsnį su *spam*, todėl Lietuvoje *spameriams* už *spam* siuntimą ar kitų su *spam* susijusių teisės normų nesilaikymą yra taikoma administracinė arba civilinė atsakomybė. Vienintelis Lietuvos Aukščiausiojo teismo išnagrinėtų bylų pavyzdys yra gana dažnai minima 2001 m. gruodžio 12 d. Lietuvos Aukščiausiojo teismo Civilinių bylų skyriaus teisėjų kolegijos priimta nutartis byloje Ž. Budros individuali įmonė „Sėkmės sistema" v. UAB "D.B.S. Ltd.Pte. Nutartyje buvo konstatuota, kad „kiekviena teisė, taip pat ir teisė perduoti informaciją šiuolaikinių telekomunikacijos priemonių pagalba, nėra absoliuti. Taigi teisė perduoti informaciją INTERNET'u nėra absoliuti ir gali būti įstatymu ribojama, jeigu toks ribojimas būtų pateisintas siekiant apginti viešą interesą, kitų asmenų teises ir teisėtus interesus. Antra vertus, teise perduoti informaciją INTERNET'u, kaip ir bet kokia kita teise, negalima piktnaudžiauti,

t.y. panaudoti subjektinę teisę priešingai jos paskirčiai, realizuojant ją neleistinomis priemonėmis ar būdais ar darant žalą kitiems asmenims.

Vienas iš piktnaudžiavimo teise atvejų naudojantis INTERNET'u yra nepageidaujamos, neprašytos komercinio pobūdžio informacijos siuntinėjimas dideliais kiekiais, kurį galima pavadinti INTERNET'o "šiukšlinimu", "teršimu" (šį reiškinį priimta apibūdinti anglų kalbos žodžiu ***spamming)***. [...].Bylą nagrinėję teismai konstatavo, kad ieškovas būtent ir siuntinėjo dideliais kiekiais komercinio pobūdžio informaciją jos nepageidaujantiems gauti asmenims [...] piktnaudžiavo savo teise perduoti informaciją ir duomenų perdavimo paslaugų sutartį atsakovas nutraukė būtent dėl paties ieškovo kaltės. Pagal ***CK 233*** straipsnį, jeigu prievolė neįvykdyta ar netinkamai įvykdyta dėl kreditoriaus kaltės, skolininkas negali būti pripažintas pažeidusiu prievolę ir jam negali būti taikoma atsakomybė."[40]

Kalbant apie teismų praktiką baudžiamosiose bylose, kuriose būtų nagrinėtas elektroninių komercinių pranešimų siuntimas. Galima būtų paminėti vieną iš bylų, kurioje spam siuntimas buvo kaip priemonė kitam nusikaltimui daryti. Tai pavyzdžiui, pagal nuteistojo E. M**.** kasacinį skundą dėl Šilutės rajono apylinkės teismo 2005 m. vasario 23 d. nuosprendžio ir Klaipėdos apygardos teismo BBS teisėjų kolegijos 2005-05-02 priimtos nutarties, kuriuo E. M. nuteistas pagal Lietuvos Respublikos ***BK 309*** straipsnio 2 dalį 3125 Lt (25 MGL dydžio) bauda. Teisėjų kolegija nustatė, kad „E. M. nuteistas už tai, kad 2003 metų spalio 27 ir 28 dienomis, turėdamas tikslą platinti, naudodamasis pasaulinio interneto tinklu, elektroniniu paštu bei jam priskirtu naudoti tarnybiniu kompiuteriu „DTK Office PC 1000 S/N (duomenys neskelbtini)", kurio IP adresas ***(duomenys neskelbtini)***, įrengtu ***(duomenys neskelbtini)***, iš savo elektroninio pašto dėžutės adresu: ***(duomenys neskelbtini)*** į A. G. elektroninio pašto dėžutę adresu: ***(duomenys nesklebtini)*** nusiuntė du elektroninio pašto laiškus, kuriuose buvo vienuolika pornografinio turinio kompiuterinių laikmenų – nuotraukų, kuriose pavaizduoti mažamečiai vaikai iki 14 metų"[41]. Šioje byloje elektroninio pašto dėžutė, iš kurios buvo siunčiami pranešimai, turintys pornografinio pobūdžio informaciją, yra laikoma priemone/ įrankiu (vienas teisės pažeidimo objektyviųjų požymių) ir nei apylinkės nei apygardos teisėjų nebuvo nagrinėjami kaip bylos esminiai klausimai. LAT BBS teisėjų kolegija nutarė panaikinti žemesnės instancijos nutartį ir perduoti nagrinėti iš naujo, nes kasatorius argumentavo, kad „211 pornografinio turinio nuotraukų jis įsigijo iki 2004 m. vasario 14 d., o už jų laikymą iki 2004 m. birželio 3 d. jis nėra nuteistas, todėl negali būti taikoma baudžiamoji atsakomybė už šių nuotraukų įsigijimą, nes to nenumatė baudžiamasis įstatymas". Svarstant teoriniame lygmenyje

[40] LAT CBS teisėjų kolegijos 2001 m. gruodžio 12 d. nutartis c.b. Ž.Budros individuali įmonė „Sėkmės sistema" v. UAB „D.B.S. Ltd.Pte", Nr. 3K-3-1326/2001 m., kat. 31.4; 37.7; 49.1

[41] LAT BBS teisėjų kolegijos 2006 m. sausio 17 d. nutartis b.b. E.M. , Nr. 2K-48/2006 m., kat. 1.2.30;2.4.2.1.

šitą situacija, būtų galima teigti, kad asmuo, gavęs tokio pobūdžio elektroninį pranešimą, greičiausiai savo teises dėl *spam* galėtų ginti tik administracine ar civiline tvarka. Pagal Lietuvos Respublikos įstatymus, tokia veika, kaip *spam* siuntimas nebūtų pripažinta teismų nusikaltimu, nes nusikaltimu pagal BK yra laikoma tik „visuomenei pavojinga veika, kuri yra aprašyta baudžiamajame įstatyme, kuria kėsinamasi į itin svarbias teisės saugomas vertybes [...].“[42] Ši nusikaltimo sąvoka puikiai atskleidžia įstatymų leidėjo poziciją, kad *spam* siuntimas Lietuvoje nėra laikomas nusikaltimu. Lietuvos Baudžiamajame kodekse nerasime įtvirtintos nuostatos, pagal kurią būtų galima kvalifikuoti tokią veiką, kaip *spam* siuntimas.

Lietuvoje nepageidaujamų elektroninių komercinių pranešimų siuntėjams, vadovaujantis Administraciniu teisės pažeidimų kodeksu (toliau – ATPK), gali būti surašomas administracinio teisės pažeidimo protokolas ir paskiriama administracinė nuobauda. Šiame kodekse yra nustatytos sankcijos už atitinkamų Reklamos įstatymo ir Elektroninių ryšių įstatymo normų pažeidimus. ATPK 189^{14} straipsnyje yra numatyta administracinė atsakomybė už įpareigojimo nutraukti įstatymų nustatytų reikalavimų neatitinkančios reklamos naudojimą ir nurodyta, kad tokiu atveju Nacionalinė vartotojų teisių apsaugos taryba gali skirti baudą nuo 500 iki 1000 litų (už pakartotinį pažeidimą – nuo 1000 iki 2000 litų). Tačiau, kaip matyti iš normos dispozicijos, pirmą kartą bauda gali būti skiriama tik tuo atveju, jei po įspėjimo *spam* ir toliau siunčiamas. Kyla klausimas, ar, turint galvoje minėto *spam* daromą žalą, egzistuojančių sankcijų dydis atitinka pažeidimo pavojingumą.

Tačiau yra keista tai, kad be minėtos sankcijos, lygiagrečiai gali būti taikomos ir kitos su tiesiogine rinkodara susijusios ATPK normos. Pavyzdžiui, ATPK 214^{14} straipsnyje yra numatyta atsakomybė už asmens duomenų tvarkymą pažeidžiant Asmens duomenų teisinės apsaugos įstatymą, o 214^{23} straipsnyje – atsakomybė už Elektroninių ryšių įstatyme numatyto asmens duomenų tvarkymo ir privatumo apsaugos pažeidimus. Pažeidimo atveju konkreti dispozicija būtų parenkama atsižvelgiant į veiklos pobūdį. Pavyzdžiui, už neteisėtą elektroninio pašto duomenų tvarkymą (pvz., tokių duomenų rinkimą ir pan.) turėtų būti taikomas ATPK 214^{14} straipsnis, tuo tarpu už patį *spam* siuntimą, pažeidžiant Elektroninių ryšių įstatymo nuostatas - 214^{23} straipsnis. „Panagrinėjus šių normų santykį su ATPK 189^{14} straipsniu galima daryti išvadą, kad pagal galiojančių normų redakcijas iš esmės skiriasi tik atsakinga institucija. Taigi, jei suinteresuotas subjektas dėl šiukšlių kreiptųsi į Nacionalinę vartotojų apsaugos tarnybą, ši pagal savo kompetenciją taikytų ATPK 189^{14} straipsnį, o jei į valstybinę duomenų apsaugos inspekciją – ši, atsižvelgusi į pažeidimo pobūdį, taikytų arba 214^{14} straipsnį, arba 214^{23}

[42] Lietuvos Respublikos Baudžiamasis Kodeksas // Žin. 1993, Nr. 12-296, Nr. 124-5626.

straipsnį. Akivaizdu, kad toks normų nenuoseklumas turėtų būti panaikintas ir tiek institucijų kompetencija, teik sankcijų sistema turėtų būti aiški.“[43]

Argentinoje už asmens duomenų apsaugą yra atsakinga „Asmens duomenų apsaugos agentūra“ (angl. *Data Protection Agency of Argentina*). Ši priežiūros institucija prižiūri, kad būtų laikomasi Asmens duomenų apsaugos įstatymo ir, vadovaudamasi šio įstatymo 31 straipsniu, taiko baudžiamąsias priemones (įspėjimą, duomenis tvarkančio asmens veiklos sustabdymą, ar skiria baudą nuo vieno tūkstančio pesų iki vieno šimto tūkstančių pesų), kai šio įstatymo nuostatos yra pažeidžiamos. Kaip jau buvo minėta, baudų dydis priklauso nuo Argentinos duomenų apsaugos agentūros priimtos dispozicijos (Disposition N^{o}. 1/2003), pagal kurią Asmens duomenų apsaugos įstatymo pažeidimai klasifikuojami į smulkius (angl. *minor,* bauda nuo 1000 iki 3000 pesų), rimtus (angl. *serious,* bauda nuo 3000 iki 50 000 pesų) ir labai rimtus (angl. *very serious,* bauda nuo 50 000 iki 100 000 pesų).

Australijos įstatymų leidėjas *Spam act of 2003* įtvirtino nuostatą, kuri numato, kad baudžiamieji procesiniai veiksmai negali būti taikomi tik dėl to, kad asmuo pažeidė civilinių nuobaudų nuostatus (angl. *civil penalty provision*), todėl pagal galiojančius Australijos įstatymus už numatytus teisės pažeidimus, kaip Lietuvoje bei Argentinoje, yra skiriamos tam tikros piniginės baudos ir restitucija, t.y. žalos atlygimas nukentėjusiajam. „Australijos komunikacijų ir medijos inspekcija“ (angl. Australian communications and media authority) – Australijos priežiūros institucija, yra atsakinga už teisės aktų nuostatų laikymąsi, o jas pažeidus, užtikrina, kad būtų vykdomos prievolės, atstatančios teisių ir pareigų vienovę.

Spam act of 2003 numatyta, kad jeigu Australijos Federalinis Teismas nutaria, kad asmuo pažeidė civilinių nuobaudų nuostatus, tai teismas asmeniui nurodo sumokėti Britanijos tautų sandraugai (angl. *the Commonwealth*) tokią piniginę baudą, kokia teismo nuožiūra bus tinkamiausia šiuo pažeidimu padarytai žalai atstatyti. Teismas, skirdamas tokią baudą, atsižvelgia į pažeidimo esmę, padarymo aplinkybes, padarymo mastą bei sukeltus nuostolius.

Maksimalios baudos skiriamos atsižvelgiant į civilinių nuobaudų nuostatuose numatytas normas, ir priklauso nuo kelių sąlygų: a) ar asmuo anksčiau buvo padaręs panašaus pobūdžio pažeidimą (pažeidimo pakartotinumas); b) ar pažeidimą padarė fizinis ar juridinis asmuo; c) ar asmuo padarė pažeidimą, numatytą šio akto 16 (1), (6) ar (9)[44] punktuose.

[43] I. Jarukaitis, T. Lamanauskas, M. Civilka ir kiti. Elektroninių ryšių teisė. – Vilnius: Eugrimas, 2005. P. 357.

[44] 16 (1) Draudžiama siųsti ar versti siųsti komercinius elektroninius pranešimus, kurie turi Australijos nuorodą ir kuriuose nėra nurodyta, jog tai komerciniai elektroniniai pranešimai [...];
16 (6) Draudžiama siųsti pranešimą neegzistuojančiais elektroniniais adresais [...];
16 (9) Asmeniui draudžiama: kurstyti, organizuoti, bendrininkauti darant pažeidimus dėl komercinių elektroninių pranešimų siuntimo be asmens sutikimo ir komercinių elektroninių pranešimų siuntimų neegzistuojančiais adresais [...].

Įstatymų leidėjas juridiniams asmenims nustato griežtesnes sankcijas už *Spam* akto pažeidimus nei fiziniams asmenims. Akte numatyta, kad jei juridinis asmuo padarė pažeidimus, numatytus 16 (1), (6) ar (9) punktuose, tuomet galima maksimali bauda yra 100 baudos vienetų, už kitų punktų pažeidimus – 50 baudos vienetų. Jei tokio pobūdžio pažeidimus padaro fizinis asmuo, tai jam atitinkamai skiriama bauda gali siekti 20 ir 10 baudos vienetų.

Jeigu Federalinis Teismas konkrečiai dienai nustato, jog vienu metu buvo padaryti 2 ir daugiau civilinių nuobaudų nuostatų pažeidimai, iš viso už tokio masto pažeidimus juridiniam asmeniui bauda gali siekti iki 2000 baudos vienetų, o už kitus pažeidimus iki 1000 baudos vienetų; atitinkamai fiziniam asmeniui - iki 400 baudos vienetų, o kitais atvejais - iki 200 baudos vienetų.

Vienos didžiausių piniginių baudų yra skiriamos juridiniams asmenims pakartotinai vykdžiusiems su *spam* susijusius pažeidimus. Pakartotinumas – sunkinanti aplinkybė. Australijos *Spam* akto 25 (5b) punktas numato, kad jei juridinis asmuo jau anksčiau buvo pažeidęs civilinių nuobaudų nuostatus, tai už pakartotinį 16 (1), (6) ar (9) punktų nuostatų pažeidimą baudžiama iki 500 baudos vienetų, o kitais atvejais iki 250 baudos vienetų. Jei Federalinis teismas nustato, kad juridinis asmuo jau anksčiau buvo pažeidęs civilinių nuobaudų nuostatus ir pakartotinai įvykdė dar 2 ar daugiau civilinių nuobaudų nuostatų pažeidimų, tai jam gali būti skiriama maksimali bauda iki 10 000 baudos vienetų už 16 (1), (6) ar (9) punktų nuostatų pažeidimus, o kitais atvejais - iki 5000 baudos vienetų.

Fiziniam asmeniui *Spam* akte yra numatytos šiek tiek švelnesnės sankcijos nei juridiniams asmenims. Federalinis Teismas gali skirti tokias maksimalias baudas: už 16 (1), (6) ar (9) punktų nuostatų pakartotinius pažeidimus baudžiama iki 100 baudos vienetų, kitais panašiais atvejais iki 50 baudos vienetų. Tačiau jei Federalinis Teismas nustato, jog pakartotinai buvo padaryti 2 ir daugiau civilinių nuobaudų nuostatų pažeidimų, tai fiziniam asmeniui gali skirti iki 2000 baudos vienetų už 16 (1), (6) ar (9) punktų nuostatų pažeidimus, o kitais atvejais - iki 1000 baudos vienetų.

Minėta Australijos komunikacijų ir medijos inspekcija 2006 m. atliko tyrimą, kurio metu buvo nustatyta, jog kompanija „Clarity1“ ir jos direktorius Wayne Mansfield nuo 2004 m., reklamuodamas savo verslą ir naudodamasis *„Business Seminars Australia and Maverick Partnership“* prekybos vardais, išsiuntė 213 milijonų komercinių elektroninių pranešimų. 2006 m. balandžio 13d. teisėja Nicholson pripažino kaltais abu: direktorių Wayne Mansfield (fizinis asmuo) ir kompaniją „Clarity1“ (juridinis asmuo) už nepageidaujamų komercinių elektroninių pranešimų siutimą ir naudojimąsi automatinių adresus renkančių programų sąrašais (angl. *using harvested address lists*). Ginamieji šiame kaltinime rėmėsi tuo, siuntėjai savo adresus buvo davę dar iki įsigaliojimo Spam act of 2003 ir suteikė galimybę gavėjams atsisakyti savo duoto

sutikimo. Teisėja šį argumentą atmetė, kuris konstatavo, kad elektroninio pranešimų gavėjų tyla ar neatsiliepimas, vadovaujantis Australijos teisės aktu, nesuteikia pagrindo laikyti, kad buvo pareikštas gavėjo sutikimas. 2006m. spalio 27 d. teisėja Nicholson kompanijai „Clarity1“ priteisė Britanijos tautų sandraugai sumokėti 4,5 milijono Australijos dolerių finansinės baudos ir kompanijos direktoriui Wayne Mansfield - 1 milijoną Australijos dolerių finansinės baudos.

Lyginant Lietuvos ir Australijos nustatytas ir nacionaliniuose teisės aktuose įtvirtintas pinigines baudas už teisės normų pažeidimus, būtų galima teigti, kad *spam* atžvilgiu Australijoje yra pasirinkta daug racionalesnė baudų skyrimo sistema nei Lietuvoje. Svarbus aspektas yra daug griežtesnių sankcijų taikymas juridiniams asmenims nei fiziniams. Pavyzdžiui, daugelyje valstybių, taip pat ir Lietuvoje, įvairios įmonės, organizacijos, siekdamos turėti geresnes pozicijas verslo rinkoje, siunčia masinius komercinius elektroninius pranešimus ir nesibaimina dėl teisės aktais nustatytų piniginių baudų, kurios dažniausiai būna mažesnės nei patiriamos kitokiomis formomis vykdomo marketingo sąnaudos. Atsižvelgiant į tai, yra svarbu nustatyti pakankamai dideles baudas, pavyzdžiui, kaip Australijoje, kad įmonės ar organizacijos savo tikslų nesiektų tokiomis neteisėtomis veiklomis. Galbūt tokiu būdu pavyktų sumažinti daromų pažeidimų, susijusių su *spam*, skaičių ne tik Lietuvoje, bet apskritai visame pasaulyje.

Išanalizavus 5 valstybių teisės aktų, reglamentuojančių *spam* sritį, nuostatas, pastebimas aiškių jurisdikcijos nuostatų nebuvimas. „Jurisdikcija nusprendžia, kurios valstybės teisė bus taikoma ir kurios valstybės teismai spręs ginčą. Atsižvelgus į pasaulinį elektroninės erdvės pobūdį valstybių teisės taikymas internete yra viena iš esminių ir iki šiol neišspręstų teisės problemų. Internete jurisdikciją sunkina tai, kad labai dažnai elektroninė informacija, prekės, paslaugos, jų teikėjas ir vartotojas yra skirtingose valstybėse ir vadovaujasi skirtingomis taisyklėmis“[45]. O kiekviena valstybė savo teisės aktuose yra įtvirtinusi teisės normas, kurios galioja tik šių valstybių teritorijose. Kyla klausimas, kurios valstybės teisės aktai turėtų galioti ir kurios valstybės teisinė atsakomybė turėtų būti taikoma, jeigu būtų siunčiamas nepageidaujamas elektroninis komercinis pranešimas (*spam)*, pvz., iš Rusijos į JAV ar iš Argentinos į Australiją. Jeigu Rusijos pilietis naudojasi kompiuteriu Rusijos teritorijoje, tai dar nereiškia, kad serveris, kuris yra naudojamas *spam* siųsti yra būtent Rusijos teritorijoje. Vienintelis Australijos *Spam act of 2003* apibrėžia teisės akto galiojimo ribas įtvirtindamas nuostatą, kad yra draudžiama siųsti elektroninius komercinius pranešimus, kurie turi Australijos nuorodą. 7 straipsnyje išsamiai nurodyta, kas yra Australijos nuoroda: *jei 1) pranešimas buvo sukurtas ir išsiųstas Australijoje; 2) individas pranešimo siuntimo metu fiziškai yra Australijoje arba pranešimo siuntimo metu organizacijos centrinė administracija ir valdyba, yra Australijoje; 3) kompiuteris ar serveris ar*

[45] M. Kiškis, R. Petrauskas, I. Rotomskis ir kt. Teisės informatika ir informatikos teisė: vadovėlis. - Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006. P. 62.

kitas įrenginys, kuris yra naudojamas prisijungimui, yra lokalizuotas Australijoje; 4) kai elektroninio pašto savininkas reziduoja Australijoje, kai pranešimas yra gaunamas į jo pašto dėžutę (jei tai fizinis asmuo, tai fiziškai yra Australijoje, jei tai juridinis asmuo, tai jo buveinė ir pagrindinė veikla turi būti vykdoma Australijoje); 5) jei pranešimas negali būti pristatytas, nes elektroninis pašto adresas neegzistuoja – laikantis nuomonės, kad toks elektroninio pašto adresas galėtų egzistuoti kaip toks ir tokiu atveju pranešimas pasiektų elektroninio pašto dėžutę naudojant kompiuterį, serverį ar kitą įrenginį, lokalizuotą Australijoje.

Atsižvelgiant į šias nuostatas pastebima, kad tradicinės jurisdikcijos požiūriu bet kurį teisinį santykį galima lokalizuoti, t.y. vadovaujantis iš anksto apibrėžtais kriterijais susieti jį su konkrečios valstybės teisės sistema. Pvz., toks susiejimas atliekamas per ginčo objektą, subjektą, veiką, papildomus kriterijus (pvz., serverio buvimo vieta). Tačiau kai kurie šio *Spam act of 2003* kritikai skeptiškai žiūri į tokį Australijos užmojį, kadangi IP adresai, domenai dažnai būna suklastoti ir neįmanoma nustatyti iš kokio serverio buvo siųsti pranešimai.

Vis dėlto vadovaujantis funkcinio lygiavertiškumo principais, jurisdikcija turėtų būti taikoma ir elektroniniams, ir įprastiems teisiniams santykiams, jei jų esmė yra tokia pati. Tarptautinė teisė pripažįsta du pagrindinius jurisdikcijos principus: pilietybės ir teritorijos, kuriais ir turėtų būti vadovaujamasi.

3. SAVIREGULIACIJA BEI TARPININKŲ VAIDMUO

Interneto turinio kontrolė yra sunkiai įmanoma dėl gana sudėtingo globalios anoniminės terpės teisinio reguliavimo, o savanoriškos elektroninės erdvės dalyvių individualių elgesio taisyklių iniciatyvos, kitaip - savireguliacija, vertinami kaip galintys duoti geresnių rezultatų. Savireguliacija – kolektyvinis reguliavimas, siekiant suderinti bendrus interesus be valstybės pagalbos. Tokia liberaliųjų pažiūrų ideologija ypač svarbi yra tose valstybėse, kuriose nėra priimtų specialiųjų teisės aktų, reguliuojančių *spam.* Savireguliacijos principu paremta veiklos priežiūra pagrįsta tam tikromis elgesio normas nusakančiomis taisyklėmis – etikos kodeksais. Šios veiklos taisyklės, kitaip etikos kodeksai, kurie tampa savireguliacijos sukurtais papročiais (*Lex mercatoria*), turėtų skatinti pasitikėjimą elektronine erdve, taip pat ir elektronine korespondencija, stiprinti, bendriems standartams nustatyti, dėl ko įvairių subjektų, pvz., IPT, veiksmai taptų nuspėjami, garantuotų atitinkamo produkto kokybę, tinkamą požiūrį į vartotoją.

Anglo – amerikietiškas teisės tradicijas puoselėjančiose šalyse įprasta kurti elgesio kodeksus, užuot didinus specializuotų įstatymų kiekį. Pastaraisiais metais tiek nacionaliniu, tiek ES, tiek tarptautiniu mastu yra skatinama rengti elgesio kodeksus, palengvinančius teisės aktų taikymą.

Kadangi visas interneto srautas perduodamas IPT tinklais, pastarųjų pažeidimas natūraliai sukelia didžiausią žalą. Dėl to IPT yra iš tų Interneto dalyvių, turinčių didžiausią suinteresuotumą dėl savireguliacijos skatinimo.

Atskirų valstybių įvairios institucijos rengia atitinkamas rekomendacijas telekomunikacijų paslaugų teikėjams ir vartotojams, kaip kovoti su nepageidaujamos informacijos platinimu, supažindina su kitų šalių taikoma sėkminga praktika. Viena dažniausiai siūlomų apsaugos priemonių siunčiamiems elektroniniams pranešimams, įtraukiama į IPT skirtas rekomendacijas – elektroninių pranešimų siunčiamo kiekio ribojimas, kurį IPT turėtų numatyti savo sutartyse ar taisyklėse. Pavyzdžiui, „*Microsoft*“ kompanija, siekdama pažaboti neprašytų elektroninių pranešimų srautus, ėmėsi konkrečių žingsnių „*Hotmail*“ sistemoje ribodama vieno vartotojo išsiunčiamų pranešimų skaičių (per parą iki 100 pranešimų). Tokią tendenciją galima pastebėti ir kai kurių Lietuvos internetinių paslaugų teikėjų taisyklėse. Tokie suvaržymai turėtų būti taikomi ne tik interneto vartotojams, bet ir kitų telekomunikacijų paslaugų vartotojams, atsižvelgiant į telekomunikacijų paslaugų teikėjų teikiamų paslaugų pobūdį ir mastą, pavyzdžiui, nustatant siunčiamų pranešimų kiekio ribojimus trumposioms SMS žinutėms, iliustruotoms žinutėms MMS ar kt. Dar vienas, jau minėtas, plačiai pasaulyje naudojamas savireguliacijos būdas - filtravimo metodai, „*do not spam*“ registrai bei „juodieji“ sąrašai. Yra rekomenduojama, kad IPT savo abonentams siūlytų filtravimo paslaugas, kurios būtų aktyvuojamos abonentui

sutikus bei turėtų blokuoti visus įeinančius pranešimus iš serverių, kurie naudojami siųsti neprašytus pranešimus („juodieji“ sąrašai), kol bus nustatytas siuntimo šaltinis. Teikiantys interneto paslaugas asmenys turėtų tikrinti ne tik elektroninį paštą priimančių serverių adresus, bet ir iš kur elektroninis pranešimas atkeliauja. Taip būtų užtikrintas kelias neprašytų pranešimų siuntinėjimui, naudojant melagingus adresus. Kaip teigiama FPK pranešime Kongresui, tokia praktika jau yra taikoma ir pasiteisinusi. IPT dažnai naudojasi susitarimu grįstais patikimumo principais, pavyzdžiui, jei yra gaunamas elektroninis pranešimas iš siuntėjo serverio, kurio patikimumą patvirtina kitas IPT, tuomet minėtas pranešimas yra priimamas į gaunančiojo serverį pagal pasitikėjimą be ypatingų filtravimo sistemų naudojimo.

Savireguliacijai plėtoti yra rekomenduojama interneto paslaugų teikėjams pažeidimų prevencijos tikslais savo pašto serverių taisyklėse įrašyti šias nuostatas:

1. Besiregistruojantys privalo suteikti teisingą ir nepasenusią informaciją apie save;

2. Nenaudoti pašto sistemos įstatymams prieštaraujančiais tikslais (pornografijos platinimui, rasinės neapykantos bei karo tematikos propagavimui);

3. Nenaudoti pašto sistemos komerciniais tikslais;

4. Nenaudoti pašto serverio masinei reklamai (*spam* siuntimui)

Gavęs nusiskundimą iš vartotojo, IPT turėtų teisę panaikinti pašto dėžutę, jei jos savininkas nusižengė naudojimosi taisyklėms. Žinoma, IPT gali paveikti pažeidėjus tik savo tinklo ribose, kitais atvejais jis gali pareikšti protestą *spamerio* IP teikėjui, išskyrus 2. punkte paminėtus atvejus (pornografijos platinimo, rasinės neapykantos bei karo tematikos propagavimo).

FPK kartu su dar 30 įvairių valstybinių institucijų iš viso pasaulio 2005 m. gegužę paskelbė projektą „*Operacija - spam zombiai*“. Šios susivienijusios tarptautinės grupės išsiuntinėjo laiškus daugiau nei 3000 IPT visame pasaulyje ir ragino tinklo specialistus ir kitus interneto dalyvius prisijungti prie pasaulinių siekių užkirsti kelią *spameriams*, keliantiems pavojų vartotojų kompiuteriams ir naudojantiems juos kaip *spam zombius*. Buvo skelbiama, kad tikslui pasiekti turi būti taikomos teisinės priemonės, techniniai pasiekimai, vartotojų ir verslininkų apmokymai (švietimas). Taip pat šiuose laiškuose, skirtuose IPT, buvo pateikiamos rekomendacijos:

„1. Blokuoti 25 prievadą, išskyrus tuos atvejus, kai jis naudojamas teisėtų pašto serverio vartotojų išsiunčiamam pranešimų srautui SMTP servisu (protokolu).

2. Kontroliuoti tempo (dažnumo) apribojimus elektroninio pašto perdavimams.

3. Identifikuoti kompiuterius, kurie siunčia neįprastus elektroninio pašto kiekius ir imtis priemonių nustatyti, ar kompiuteris veikia kaip „spam zombis“. Jeigu būtina, izoliuoti apkrėstą kompiuterį tol, kol nebus pašalintas probleminis šaltinis.

4. Patarkite savo klientams suprantama kalba, kaip apsaugoti jų kompiuterius nuo virusų, Trojos arklių (angl. *Trojans*) ar kitų neigiamų reiškinių, kurie paverčia kompiuterį „spam zombiu“, ir suteikti šiam tikslui reikalingą pagalbą, priemones.

5. Suteikite savo klientams lengvai įgyvendinamas priemones *zombio* kodui pašalinti, jeigu jų kompiuteriai buvo apkrėsti, ir suteikite reikalingą pagalbą.“[46]

Kita sritis, kurią, ypač JAV, IPT reguliuoja, tai jau minėtos pornografijos ir kitų suaugusiems skirtų pranešimų ribojimas ir išskirtinis pateikimas. IPT siūlo galimybę blokuoti tam tikrus vaizdus, kurie yra pateikiami elektroninio pašto pranešimuose. Užuot įterpę vaizdą tiesiogiai įprasto elektroninio pašto pranešimo turinyje, elektroninio pašto pranešimų siuntėjai dažniausiai laiko šiuos vaizdus interneto serveryje. Gavėjui atsidarius pranešimą, elektroninio pašto programa parsiunčia šiuos vaizdus iš interneto serverio taip, kad juos būtų galima matyti elektroniniame pranešime. Siekdami apsaugoti nuo tokio automatinio, pvz., pornografinių vaizdų persiuntimo, IPT ir elektroninio pašto programos naudoja vaizdų blokavimo programą, sustabdančią šį procesą. Daugelis IPT daro tai specialiai, jeigu nustato, kad pranešimas turi *spam* požymių.

Kita vartotojų apsaugos priemonė, kuri teisės aktuose nėra įtvirtinta, bet IPT dažnai naudojama, siekiant apsaugoti nuo automatiškai elektroninio pašto dėžutes kuriančių kompiuterinių programų, tai tam tikrų ženklų atkartojimas, skaičių įvedimas ar veiksmų privalomos sekos atlikimas, kuriuos suprasti ir įvykdyti geba tik žmogaus protas. Tokiu būdu IPT bando apsaugoti nuo *spamerių* sukurtų programų, kurios „keliauja“ internete ir automatiškai kuria elektroninio pašto dėžutes su tikslu ateityje išsiųsti *spam*.

Vis dėlto IPT yra numatytos ne tik minėtos teisės plėtojant savireguliaciją *spam* atžvilgiu. Kaip viena iš *spam* problemos poveikio priemonių yra IP teikėjams numatytos tam tikros pareigos - padėti užtikrinti internete platinamos informacijos saugumą, tam tikrų priemonių naudojimą prieš nelegalų *spam* platinimą. Kai kurių valstybių įstatymai numato atsakomybę IPT už šių pareigų nevykdymą. Pavyzdžiui, išskirtinai didelės apimties Australijos 1997 m. Telekomunikacijų įstatymas išsamiai reglamentuoja IPT paslaugų teikimo sąlygas, taisykles, atsakomybę, skatina savireguliaciją bei industrijos kodeksų kūrimą.

ES galiojančioje Elektroninės komercijos direktyvoje, kurios nuostatos perkeltos ir į Lietuvos teisės aktus, nustatyta, kad „Norėdamas pasinaudoti atsakomybės apribojimu, informacinės visuomenės paslaugos, kurią sudaro informacijos saugojimas, teikėjas, gavęs faktinių žinių arba sužinojęs apie neteisėtą veiklą, privalo nedelsdamas imtis priemonių panaikinti tą informaciją arba atimti galimybę ja naudotis; informacija turi būti panaikinta arba

[46] Operation spam zombie // http://www.ftc.gov/bcp/conline/edcams/spam/zombie/translations/lithuanian.pdf; prisijungimo laikas : 2008-07-02.

galimybė ja naudotis turi būti atimta vadovaujantis saviraiškos laisvės principu ir šiam tikslui nacionaliniu lygiu nustatyta tvarka“ [47].

ES elektroninės komercijos direktyva 12, 13 ir 14 straipsniuose nustato, kad informacinės visuomenės paslaugų teikėjas nėra atsakingas už perduodamą informaciją, laikiną jos saugojimą (angl. *caching*) ar apskritai informacijos turinį, jei pats neinicijuoja perdavimo, neparenka informacijos gavėjo, neparenka ir nepakeičia perduodamos informacijos, laikosi prieigos prie informacijos sąlygų.

Elektroninės komercijos direktyvos 15 str. įtvirtina nuostatą, kad „valstybės narės neturi nustatyti teikėjams nei bendros prievolės teikiant 12, 13, 14 str. reglamentuojamas paslaugas stebėti informaciją, kurią jie perduoda arba saugo, nei bendros prievolės aktyviai domėtis faktais arba aplinkybėmis, rodančiomis nelegalią veiklą“. Direktyva nustato gaires, kad informacinės visuomenės paslaugų teikėjams būtų prievolė nedelsiant informuoti kompetentingas viešąsias institucijas apie įtariamą nelegalią veiklą arba informaciją, kurią pateikia jų paslaugų gavėjai arba pateikti šių gavėjų tapatybę. Taigi ir direktyvos kūrėjai palieka šią sritį daugiau savireguliacijai.

Komercijos direktyva valstybėms narėms palieka teisę nustatyti specifinius reikalavimus, kuriuos reikia nedelsiant patenkinti prieš panaikinant informaciją arba atimant galimybę ją pasiekti.

Elektroninės komercijos direktyva iš valstybių narių neatima galimybės reikalauti, kad paslaugų teikėjai, internete pateikiantys paslaugos gavėjų perduotą informaciją, laikytųsi įsipareigojimų, kurių galima pagrįstai tikėtis ir kurie nurodyti nacionalinėje teisėje, su informacija elgtis rūpestingai, tam, kad būtų atskleista tam tikrų rūšių neteisėta veikla ir jai būtų užkirstas kelias. Direktyvoje nurodyta, kad valstybės narės ir Komisija turės skatinti rengti elgesio kodeksus; taip nebus pakenkta savanoriškam tokių kodeksų pobūdžiui ir nebus siekiama riboti galimybės suinteresuotosioms šalims laisvai spręsti, ar laikytis tokių kodeksų.

Argentinos ***anti-spam*** įstatymo projekte yra siekiama įtvirtinti nuostatą, kurioje būtų numatyta bauda nuo 3000 pesų iki 100 000 pesų tiems, kas siuntė ar padėjo siųsti nelegalius elektroninius pranešimus. Įstatymo projekte numatyta, kad šios sankcijos taikomos ir IPT, kurie žinodami apie siekį išsiųsti nelegalius elektroninius pranešimus, vis tik leidžia klientams naudotis jų paslaugomis. Baudos dydis priklauso nuo pažeidimo tipo, gavėjų kiekio ar pakartotinumo.

Jau minėta, kad Rusijoje neformali interneto paslaugų teikėjų asociacija OFISP sukūrė interneto vartotojų elgesio kodeksą OFISP – 008, kuris sukurtas remiantis verslo

[47] Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1.

taisyklėmis. Jame yra numatyta, kad *spameriai* pažeisdami šį dokumentą, pažeidžia ir Rusijos Federacijos civilinės teisės įstatymus. Tai sudaro pagrindą Interneto teikėjams, kurie teikia prieigą prie Interneto, nutraukti sutartis su *spameriams*.

Kitas *spam* problemos sprendimo būdas savireguliacijos aspektu – vartotojų savisauga. Pasaulyje valstybinių institucijų, kovojančių prieš nelegalųjį *spam*, teikiamose rekomendacijose, informuojama, kad kiekvienas internetinių paslaugų vartotojas turėtų rūpintis savo paties saugumu ir prieš suteikdamas savo asmens duomenis svetainėms (elektroninio pašto adresą ir pan.) turėtų įsitikinti, ar bus užtikrintas jo privatumas, ir laikytis šių reikalavimų:

a) „niekuomet nesinaudoti programomis, kurios buvo gautos elektroniniu paštu, prieš tai neįsitikinus, kad jos neužkrėstos virusais [...].

b) jei elektroninis paštas tikrinamas iš bibliotekų, mokymo įstaigų ar kitų viešųjų vietų, užbaigus darbą reikėtų uždaryti naršyklę. Jei yra galimybė, papildomai reikėtų ištrinti slapukus (*cookies*), nes pagal slapukus neprašytų žinučių siuntėjai sprendžia apie vartotojų pomėgius (automobiliai, elektroninės prekės, nekilnojamas turtas ir pan.) ir prieš siųsdami vartotojams neprašytas žinutes jas atitinkamai klasifikuoja;

c) prieš siųsdamas kompanijai savo nesutikimą dėl gaunamų neprašytų žinučių, vartotojas turėtų įsitikinti, kad kompanija patikima, nes priešingu atveju tik bus išsiųstas patvirtinimas, kad šis adresas tikras (ko ir siekia *spam* platintojai)“[48].

Tiesiogine rinkodara užsiimančios kompanijos klientai, naudojantys elektroninio pašto paslaugas, įskaitant SMS ir MMS vartotojus, elektroninio pašto paslaugų teikėjai, įskaitant judriojo ryšio paslaugų teikėjus, turėtų būti informuojami apie naujas taisykles, būdus ir metodus, kaip apsisaugoti nuo neprašytų komercinių žinučių, apie skundų priėmimo tvarką, kaip kovoti su nepageidaujamos informacijos platinimu žinutės išsiuntimo metu (rekomendacijos ne tik paslaugų teikėjams, bet ir telekomunikacijų operatoriams).

Analizuojant *spam* reiškinį pastebėta, kad reikalingos ne tik teisinės apsaugos priemonės, bet labai svarbu, kad ir IPT, ir elektroninio pašto vartotojai atsargiai elgtųsi su asmeniniais elektroninio pašto adresais, kurie yra paklausi prekė internete. Kiekvienam vartotojui elektroninio pašto adresą derėtų saugoti kaip asmens kodą. Kaip teigia Ryšių reguliavimo tarnybos atstovai, „mąstyk globaliai, veik lokaliai“. Nors problema, aišku, yra globali, kiekvienas iš mūsų pirmiausiai turėtų pradėti veikti lokaliai - nuo savo elektroninio pašto dėžutės, IPT – atitinkamai turėtų veikti savame elektroninių ryšių tinkle, valstybės institucijos - nacionaliniu lygiu.

[48] Rekomendacijos „Ką daryti norint atsisakyti nepageidaujamų elektroninių žinučių?“ // http://www.ada.lt/images/cms/File/rekomendacijos_del_el_zinuciu.pdf; prisijungimo laikas: 2008-11-10.

Tokiu būdu suderinus teisines apsaugos priemones su atitinkamomis pačių vartotojų galimomis apsaugos priemonėmis, būtų galima tikėtis efektyvių pokyčių kovojant su *spam* reiškiniu.

4. SPAM PROBLEMOS EMPIRINIS TYRIMAS „*SPAM* TEISINIS REGULIAVIMAS PRAKTINIU LYGINAMUOJU ASPEKTU: PRAKTINĖS *SPAM* LAIŠKŲ ATSISAKYMO PROBLEMOS“

4.1. Empirinio tyrimo „*Spam* teisinis reguliavimas praktiniu lyginamuoju aspektu: praktinės *spam* laiškų atsisakymo problemos“ programa

Problema. Nors elektroniniai komerciniai pranešimai ir jų siuntimas daugelyje šalių yra reglamentuoti, tačiau teisės pažeidimų atvejų dėl *spam* vis daugėja.

Tikslas. Padėti atskleisti magistro baigiamojo darbo „*Spam* teisinis reguliavimas – lyginamasis aspektas“ tikslą ir patvirtinti teorines išvadas empiriškai išnagrinėjant ir patikrinant, ar užsakomi ir gaunami elektroniniai komerciniai pranešimai atitinka Lietuvos, JAV, Rusijos, Argentinos ir Australijos teisės aktų numatytus reikalavimus.

Uždaviniai:

1. Atlikti pasirinktų valstybių (Lietuvos, JAV, Rusijos, Argentinos ir Australijos) teisės aktuose elektroniniams pranešimams keliamų reikalavimų, jų panašumų ir skirtumų lyginamąją analizę.

2. Kiekvienoje analizuojamoje valstybėje sukūrus po eksperimentinę elektroninio pašto dėžutę (bus galima spręsti pagal domeno pabaigą pvz., „ .lt“ ar „ .ru“), empiriškai patikrinti ir ištirti, ar elektroninių komercinių pranešimų siuntėjai laikosi valstybių (kuriose įsteigtas tas paslaugų tiekėjas) norminių teisės aktų siunčiamo pranešimo turinio ir asmens duomenų apsaugos atžvilgiu.

3. Neatsižvelgiant į *opt-in* (išankstinio sutikimo taisyklė) ir *opt-out* (atsisakymo taisyklė) valstybių teisės aktuose įtvirtintus pranešimų gavimo ir atsisakymo metodus, išanalizuoti tolimesnius pranešimų siuntėjų (duomenų valdytojų) veiksmus, kai siekiama atsisakyti jų siunčiamų elektroninių komercinių pranešimų, ir įvertinti elektroninio pranešimo atsisakymo sudėtingumą.

4. Atsižvelgiant į tyrimo rezultatus, surinkti statistinius duomenis ir juos įvertinus, atlikti lyginamąją analizę bei pateikti efektyvaus teisinio reglamentavimo ir įgyvendinimo modelį.

Numatomas objektas: tiriamų 5 valstybių (Lietuvos, JAV, Rusijos, Argentinos, Australijos) teisės aktais apibrėžtų reikalavimų laikymasis elektroniniuose komerciniuose pranešimuose.

Dalykas: elektroniniai komerciniai pranešimai (spam).

Hipotezė. Daugiausiai pažeidimų dėl pranešimų turinio, jų rekvizitų, siuntimo bei atsisakymo bus padaryta tose valstybėse, kuriose nėra priimtų specialiųjų *anti-spam* teisės aktų, kurie detaliai reglamentuotų elektroninius pranešimus.

Tyrimo etapai:

1 etapas: teisės aktų Lietuvoje, JAV, Rusijoje, Argentinoje, Australijoje *spam* atžvilgiu analizė (iš dalies ją išnagrinėjus magistro baigiamojo darbo dėstomojoje dalyje).

2 etapas: eksperimentinių elektroninių pašto dėžučių sukūrimas Lietuvoje, JAV, Rusijoje, Argentinoje, Australijoje.

3 etapas: elektroninių komercinių pranešimų užsakymas ir jų monitoringas (nuo pranešimų užsakymo dienos stebima 3 savaites).

4 etapas: gaunamų elektroninių komercinių pranešimų atsisakymo proceso vykdymas ir duomenų valdytojo elgsenos stebėjimas po pareikšto atsisakymo gauti pranešimus (3-4 savaitės).

5 etapas: gautų duomenų analizė ir empirinio tyrimo išvadų pateikimas.

Tyrimo metodai : 1) teisinių dokumentų analizė; 2) eksperimentas.

Tyrimo naujumas, reprezentatyvumas, reikšmė. *Spam* problema yra aktuali ne tik Lietuvoje, bet ir visame pasaulyje. Remiantis statistiniais duomenimis, *spam* yra vienas iš dažniausiai elektroninėje erdvėje vykdomų teisės pažeidimų. (priedas Nr. 1). Šio empirinio tyrimo metu gauti duomenys turėtų atskleisti teisės aktų įtaką *spam* reiškiniui. Tyrimas turėtų parodyti, ar yra laikomasi teisės aktuose keliamų reikalavimų. O gal teisės normos yra tik teorinio pobūdžio ir pagrindinį vaidmenį atlieka savireguliacija. Tyrimas, su kokiais sunkumais susiduria elektroninio pašto savininkas- vartotojas. Tyrimo metu gauti duomenys, turėtų atsakyti į klausimus, ar nustatytos teisės normos yra reikšmingos siekiant apsaugoti vartotoją nuo brukamos reklamos, ar pakankamai efektyvios yra prevencinės priemonės – sankcijos.

Spam empirinis tyrimas teisiniu lyginamuoju aspektu Lietuvoje nebuvo atliktas.

Siekiant kuo didesnio reprezentatyvumo, tyrimui pasirinktos 5 valstybės iš skirtingų pasaulio kontinentų. Tiriamų valstybių elektroniniame pašte bus užsisakomi vienodo pobūdžio elektroniniai komerciniai pranešimai iš 4 skirtingų sričių:

1. 2-jų skirtingų kelionių agentūrų komerciniai pranešimai;
2. 2-jų skirtingų naujienų agentūrų komerciniai pranešimai, kuriuose pateikiama svarbiausios pasaulio apžvalgos iš ekonomikos, finansų srities;
3. 2-jų skirtingų suaugusiems skirtų interneto puslapių siunčiami informaciniai ir komerciniai pranešimai;
4. 2-jų IT prekių elektroninių parduotuvių komerciniai pranešimai.

Tyrimo metu bus stebima, ar duomenų valdytojai nepiktnaudžiaus jiems pateiktais duomenimis (elektroninio pašto adresais) ir neperduos jų kietiems duomenų valdytojams. Kadangi JAV ir Argentinoje įtvirtintas *opt-out* (liet. atsisakymo) metodas, tyrimo metu į sukurtą elektroninį paštą gali būti gaunami ir kitokio pobūdžio neužsakyti komerciniai pranešimai, kurie tokiu atveju irgi paklius į tyrimo ribas.

4.2. Tyrimo eiga, rezultatai ir išvados

I. etapas. Laikantis tyrimo programos, kuri parengta vadovaujantis Mykolo Romerio universiteto Senato 2002 m. gruodžio 21d. nutarimu Nr. 1SN-37 patvirtintais metodologiniais nurodymais, 1 tyrimo etapas - teisės aktų Lietuvoje, JAV, Rusijoje, Argentinoje, Australijoje *spam* atžvilgiu analizė – buvo įgyvendintas ir aprašytas magistro baigiamojo darbo dėstomojoje (teorinėje) dalyje. Šios analizės santrauka pateikiama priede Nr. 5.

II etapas. 2008-09-26 buvo pradėtas įgyvendinti antrasis empirinio tyrimo etapas, t. y., 5 skirtingose nagrinėjamose valstybėse (Lietuvoje, JAV, Rusijoje, Argentinoje, Australijoje) sukurtos 5 eksperimentinės elektroninio pašto dėžutės, kurių priklausomybę atitinkamai valstybei galima atpažinti pagal domenų pabaigas („ .lt“- Lietuvos; „ .com“- JAV):

1. 2008-09-26 sukurta Lietuvoje – vardene.pavardene@inbox.lt;
2. 2008-09-26 sukurta JAV – vardene.pavardene@mail.com;
3. 2008-10-06 sukurta Rusijoje – vardene.pavardene@rambler.ru;
4. 2008-09-22 sukurta Argentinoje – vardene.pavardene@cuidad.ar;
5. 2008-10-02 sukurta Australijoje – vardene.pavardene@inthemix.com.au.

III etapas. Sukūrus elektroninio pašto dėžutes, reikalingas eksperimentui atlikti ir empirinio tyrimo tikslui siekti, buvo užsakyti elektroniniai komerciniai pranešimai (empirinio tyrimo dalykas. Eksperimento metu į 5 elektroninio pašto dėžutes iš viso buvo užsakyti 40-ties skirtingų įmonių informaciniai naujienlaiškiai ar prekes ir paslaugas reklamuojantys komerciniai pranešimai, t.y. į tiriamų valstybių elektroninį paštą buvo užsakyti vienodo pobūdžio elektroniniai komerciniai pranešimai iš 4 skirtingų sričių: 1) kelionių agentūrų; 2) naujienų agentūrų; 3) suaugusiems skirtų internetinių puslapių; 4) IT prekių elektroninių parduotuvių.

Pateikiant eksperimento rezultatus buvo siekiama konfidencialumo, nes

a) įmonės, kurių užsakyti ir atsiųsti pranešimai buvo įtraukti į šį eksperimentą, apie eksperimentą nebuvo įspėtos;

b) registruojantis dėl elektroninių komercinių pranešimų gavimo nebuvo pateikiami tikri gavėjo (pranešimų užsakovo) duomenys (tikras buvo tik elektroninio pašto adresas).

Pateikiame III tyrimo etapo, kuris truko keturias savaites, rezultatus (Priedas Nr. 6, 1-5 lentelės):

1. Į sukurtas 5 elektroninio pašto dėžutes iš viso buvo gauta 351 elektroninis laiškas iš skirtingų 45 adresantų (siuntėjų):

a) į Lietuvoje sukurtą elektroninio pašto dėžutę gauti 83 laiškai;

b) į JAV sukurtą elektroninio pašto dėžutę gauti 66 laiškai;

c) į Rusijoje sukurtą elektroninio pašto dėžutę gauti 50 laiškų;

d) į Argentinoje sukurtą elektroninio pašto dėžutę gauti 81 laiškas;

e) į Australijoje sukurtą elektroninio pašto dėžutę gauti 71 laiškas.

2. Buvo gauti 5 neužsakyti laiškai iš 5 adresantų: į Lietuvos elektroninio pašto dėžutę buvo gauti 3 laiškai, į JAV – 1 laiškas, į Rusijos – 1 laiškas.

3. pagal sritis buvo gauta:

a) 105 pranešimai iš kelionių agentūrų;

b) 187 pranešimai iš naujienų agentūrų;

c) 22 pranešimai iš suaugusiems skirtų portalų;

d) 32 iš IT elektroninių parduotuvių;

4. Gauti 5 neužsakyti pranešimai: 1 - iš suaugusiems skirto portalo, 1 - iš internetinio lažybų punkto, 1 – kvietimas prisijungti prie vienos internetinių pokalbių svetainės ir 2 iš nekilnojamojo turto agentūrų.

5. Į Lietuvos elektroninio pašto dėžutę vardene.pavardene@inbox.lt buvo gauta 80 užsakytų pranešimų, iš kurių 63 atitiko Lietuvos teisės aktus. Iš 2 Lietuvos įmonių buvo gauta 17 elektroninių komercinių pranešimų, kurie neatitiko Lietuvoje teisės aktų keliamų reikalavimų, t.y. nebuvo pateikta jokios nuorodos ar informacijos apie tai, kaip galima atsisakyti elektroninių pranešimų. Remiantis įstatymo nuostatomis, nebuvo sudaryta „lengvai įgyvendinama galimybė nemokamai ir paprastomis priemonėmis“ atsisakyti komercinių pranešimų. Minėti pranešimai atsiųsti iš naujienų agentūros ir suaugusiems skirto portalo. Į šį skaičių neįtraukti pranešimai, atsiųsti be išankstinio užsakymo.

6. Į JAV elektroninio pašto dėžutę vardene.pavardene@mail.com buvo gauti 65 užsakyti komerciniai pranešimai. Iš 2 JAV siuntėjų atsiųsti 5 elektroniniai pranešimai neatitiko JAV *Can spam* akto keliamų reikalavimų:

a) iš suaugusiems skirto portalo atsiųstų komercinių pranešimų antraštė neinformavo, jog pranešimas „skirtas suaugusiems“ ar turi „seksualiai atviro“ pobūdžio tyrinį. (šie pranešimai turėjo teisingai informuojančią antraštę, kurioje nurodytas siuntėjo pavadinimas ir reklamuojamų prekių ar paslaugų pobūdis);

b) abiejų siuntėjų atsiųstuose pranešimuose nebuvo pateikti siuntėjų fiziniai adresai;

c) vieno siuntėjo pranešimai neturėjo „atsisakymo“ (angl. „*unsubscribe*“) mechanizmo.

7. Į Rusijos elektroninio pašto dėžutę vardene.pavardene@rambler.ru buvo gauti 49 elektroniniai pranešimai. Nustatyta, kad visi pranešimai turėjo antraštę, kurioje nurodytas siuntėjo pavadinimas ir trumpas pranešimo turinio apibūdinimas. Iš 4 siuntėjų gauti 13 pranešimų neturėjo atsisakymo mechanizmo, 6 siuntėjai iš 8 nenurodė fizinio adreso, 6 siuntėjai iš 8 nepateikė jokios informacijos apie save (tačiau pagal Rusijos Federacijoje galiojančius teisės aktus yra nereikalaujama pateikti informacijos apie siuntėją, atsiskaymo mechanizmą bei fizinį siuntėjo adresą).

8. Į Argentinos elektroninio pašto dėžutę vardene.pavardene@cuidad.ar buvo gautas 81 pranešimas. Visi pranešimai turėjo „atsisakymo“ mechanizmą, atgalinį adresą ir teisingas antraštes, 77 nebuvo įtrauktas fizinis siuntėjo adresas, 49 nebuvo įtraukta informacija apie siuntėją (tačiau pagal Argentinoje galiojančius teisės aktus yra nereikalaujama pateikti šios informacijos).

9. Į Australijos elektroninio pašto dėžutę vardene.pavardene@inthemix.com.au buvo gautas 71 pranešimas. Visi pranešimai turėjo „atsisakymo“ mechanizmą, atgalinį adresą ir teisingas antraštes. 21 pranešime nebuvo fizinio siuntėjo adreso, 4 nebuvo pateikta jokios informacijos apie siuntėją.

10. Kiti empirinio tyrimo III etapo duomenys:

a) visi užsakyti pranešimai turėjo atgalinį adresą,

b) 316 pranešimų turėjo „atsisakymo“ mechanizmą,

c) į 113 pranešimų buvo įtrauktas siuntėjo fizinis adresas,

d) 17–oje pranešimų buvo nurodytas ne fizinis adresas, o anoniminė pašto dėžutė, kurioje pateikiamas tik jos numeris.

e) nė vienas suaugusiems skirtas pranešimas neturėjo specialių, išsiskiriančių ir įspėjančių ženklų, kurie informuotų apie seksualinio pobūdžio pranešimo turinį.

f) visi 5 gauti neužsakyti pranešimai turėjo atgalinį adresą, tačiau nė viename iš jų nebuvo nurodyta, kaip galima jų atsisakyti. Į elektroninio pašto dėžutes, turinčias Lietuvos ir Rusijos domenų pabaigas, gauti 4 pranešimai (3 Lietuvoje ir 1 Rusijoje) gali būti laikomi ***spam***, nes šios šalys laikosi ***opt-in*** metodo (negalima siųsti pranešimų be išankstinio adresato sutikimo). Vienas neužsakytas pranešimas, gautas į JAV elektroninio pašto dėžutę, laikomas teisėtu, nes šios valstybės teisės aktuose įtvirtintas ***opt-out*** metodas.

IV etapas. Praėjus 4 savaitėms po elektroninių komercinių pranešimų užsakymo, buvo pradėtas vykdyti IV empirinio tyrimo etapas: pranešimų atsisakymas ir šios procedūros sudėtingumo vertinimas, kuris skirstomas pagal šiuos kriterijus:

- nesudėtingas (N) – jei pranešime yra pateikta informacija apie pranešimo atsisakymo žingsnius ar nuoroda, kurią paspaudus pranešimo pavyksta atsisakyti iš karto.

- sudėtingas (S) – jei pranešime nėra pateikta jokios pranešimo atsisakymo informacijos ar nuorodos, tačiau, išsiuntus prašymą siuntėjo nurodytu atgaliniu adresu nebesiųsti pranešimų, jis buvo patenkintas iš pirmo karto;

- labai sudėtingas (LS) - jei pranešimo nepavyksta atsisakyti iš antro ar trečio karto.

Įgyvendinus IV empirinio tyrimo etapą, gauti rezultatai:

Šalis	**Nesudėtingai atsisakyta**	**Sudėtingai atsisakyta**	**Labai sudėtingai atsisakyta**
Lietuva	6	1	1 naujienų agentūros (+12 pranešimų)
JAV	7	1	-
Rusija	3	3	2 naujienų agentūrų (+6 ir + 4 pranešimai)
Argentina	7	-	1 kelionių agentūros (+13 pranešimų)
Australija	7	-	1 naujienų agentūros (+ 3 spam)
Iš viso	**30**	**5**	**5** agentūrų (+ 38 pranešimai)

1. nesudėtingai atsisakyta 30 siuntėjų siunčiamų elektroninių pranešimų:
    a) Lietuvoje – 6 iš 8
    b) JAV – 7 iš 8
    c) Rusijoje – 3 iš 8
    d) Argentinoje – 7 iš 8
    e) Australijoje - 7 iš 8
2. sudėtinga atsisakyti buvo 5 iš 40 siuntėjų siunčiamų elektroninių pranešimų:
    a) Lietuvoje - 1
    b) JAV -1;
    c) Rusijoje – 3
3. Laikoma, kad labai sudėtinga buvo atsisakyti 5 iš 40 siuntėjų siunčiamų pranešimų:

a) Lietuvoje – 1 siuntėjo (naujienų agentūros). Atsisakius pirmą kartą gauta dar 12 nepageidautų pranešimų (*spam*) į elektroninio pašto dėžutę. Visų pranešimų galutinai atsisakyti pavyko iš antro karto;
b) Rusijoje – 2 siuntėjų (2 naujienų agentūrų). Atsisakius pirmą kartą, viena naujienų agentūra atsiuntė dar 6 nepageidaujamus pranešimus, kita – 4. Iš viso gauta 10 *spam*. Visų pranešimų galutinai atsisakyti pavyko iš antro karto;
c) Argentinoje - 1 siuntėjo (kelionių agentūros). Atsisakius pirmą kartą gauti 9 nepageidaujami pranešimai. Pakartojus atsisakymo procedūrą antrą kartą gauti dar 4 pranešimai. Nepageidaujamų pranešimų galutinai atsisakyti pavyko tik iš trečio karto.

V etapas. Išanalizavus 5 pasirinktų valstybių teisės aktus ir atlikus empirinį tyrimą, būtų galima patvirtinti dar prieš tyrimą iškeltą hipotezę. Eksperimento duomenys parodė, kad tose valstybėse, pvz., Rusijoje, Argentinoje, Lietuvoje, kuriose nėra priimti specialūs *anti spam* teisės aktai ir nėra teisės normų, detaliai reglamentuojančių elektroninių komercinių pranešimų siuntimą, pranešimų turinį ir jo rekvizitus, yra dažniau pažeidžiamos elektroninio pašto vartotojų teisės nei JAV ar Australijoje. Eksperimentas parodė, kad tų valstybių pranešimų siuntėjai, kuriems neprivalomas „atsisakymo“ mechanizmo (pvz., aktyvios nuorodos „atsisakyti čia“ ar instrukcijos, paaiškinančios kaip atsisakyti pranešimų) įtraukimas į elektroninį pranešimą, jo ir neįtraukė. IV empirinio tyrimo etapo metu pastebėta, kad daugiausiai (3 iš 6) nepavyko atsisakyti tų siuntėjų siunčiamų pranešimų, kuriuose nebuvo pateiktas aiškus pranešimų atsisakymo mechanizmas, neįtraukta informacija apie siuntėją bei fizinis adresas. Galima daryti išvadą, kad tose valstybėse, kuriose nėra priimti specialieji *anti spam* teisės aktai ir detaliai reglamentuotas elektroninių (komercinių) pranešimų siuntimas, buvo padaryta daugiausiai pažeidimų, to pasekmė – vartotojo teisių ir interesų pažeidimai. *Spameriai* dažniausiai ir naudojasi tokiomis teisės spragomis ir naudoja tų valstybių elektroninio pašto dėžutes bei kompiuterius *spam* siųsti.

IT apsaugos ir kontrolės firmos „*Sophos*“ pateiktais nepriklausomais duomenimis (Priedas Nr. 7), paskutiniu metu pasaulyje pastebimas spartus *spam* atakų antplūdis iš Rusijos bei Argentinos. 2008 metų I ketvirtį pasaulyje daugiausiai *spam* buvo išsiunčiama iš JAV (daugiau nei 15 proc.) bei Rusijos (beveik 8 proc.), o žvelgiant atskirai pagal kontinentus, daugiausiai *spam* atakų vykdoma iš Azijos kontinento (34,3 proc.), Europos (30,7 proc.) bei Šiaurės Amerikos(18,9 proc.)[49]. Šie nepriklausomų statistikos agentūrų surinkti duomenys iš dalies patvirtina atlikto eksperimento duomenis.

[49] Sophos Security threat report update 07/2008 // www.sophos.com/news/2008/07/dirtydozjul08.html; prisijungimo laikas: 2008-10-10.

IŠVADOS IR PASIŪLYMAI

1. Atlikus ***spam*** reiškiniui būdingų bruožų analizę, nustatyti du ***spam*** suvokimo aspektai:

- (siaurąja prasme) tai nepageidaujamas elektroninis komercinis pranešimas, kurį siunčia įmonės rinkodaros, marketingo, komerciniais, reklamos tikslais;
- (plačiąja prasme) tai masiškai siunčiamas nepageidaujamas elektroninis pranešimas, kurio turinys nebūtinai yra komercinis, tačiau gali būti kenkėjiško arba amoralaus pobūdžio, arba yra skirtas sukčiams gauti materialinės naudos, arba visiškai beprasmio turinio pranešimas, kurio tikslas – apkrauti interneto tinklus.

2. Atlikus Lietuvos, JAV, Australijos, Argentinos ir Rusijos valstybių teisės aktuose įtvirtintų ***spam*** reguliuojančių teisės normų analizę, nustatyta, kad:

- nėra vieningos ***spam*** sąvokos ir tesės aktuose yra skirtingai traktuojamas ***spam*** terminas;
- nėra vieningo tarptautinio sutarimo dėl ***spam*** platinimo priemonių, kurios suteikia galimybę ***spam*** siuntėjams naudoti ne tik internetą, bet ir kitas alternatyvias priemones. Vienose valstybėse (pvz., Rusija) ***spam*** platinimo priemone laikomas tik internetas ir mobilusis telefonas, kitose, be jau minėtų, – internetas, mobilusis telefonas, faksimiliniai aparatai, pranešimų gavikliai (pvz., JAV, Australija) bei automatinio skambinimo sistemos be žmogaus įsiterpimo - skambinimo automatai (Lietuva (ES)), dar kitose (pvz., Argentina) - apskritai nėra nieko įvardijama;
- yra akcentuojamas elektroninių pranešimų komercinis pobūdis, tačiau nei viena nagrinėta valstybė į savo teisės aktuose pateikiamą ***spam*** sąvoką nėra įtraukusi ir reglamentavusi ne komercinės paskirties elektroninių pranešimų, nors darbe analizuojant ***spam*** sampratą pastebėta, kad daugelis šių valstybių savo tarptautiniuose pranešimuose, konferencijose bei atsakingų institucijų metinėse ataskaitose ***spam*** pateikia ir nagrinėja plačiąja prasme;
- kiekviena valstybė reglamentuoja elektroninių komercinių pranešimų siuntimą ir laikosi savo teisėje įtvirtinto ***sutikimo (***angl. ***„opt-in“*** - Lietuva, Australija, Rusija) arba ***atsisakymo*** (angl. ***„opt-out“*** – JAV, Argentina) metodo, tačiau dėl šių skirtingų metodų taikymo atsirado terpė platinti ***spam;***
- egzistuoja didelė įvairių valstybių teisės aktų ir juose įtvirtintų reikalavimų elektroniniams komerciniams pranešimams įvairovė, tad elektroninio pašto pranešimų siuntėjui, besinaudojančiam viena globalia interneto erdve, yra sunku susiorientuoti ir gana dažnai padaromi ***spam*** pažeidimai; tačiau teisėje įtvirtinta nežinojimo prezumpcija teigia, kad įstatymų nežinojimas – neatleidžia nuo atsakomybės;

- už internete – vienoje globalioje erdvėje – padarytą tokio paties pobūdžio teisės pažeidimą, *spam* platinimą, atskirose valstybėse taikomos ne tik skirtingo dydžio piniginės baudos (pvz., Lietuvoje juridiniam asmeniui už pakartotinį *spam* platinimą maksimali piniginė bauda yra 2000 Lt, Rusijoje ji yra 2, Argentinoje – 38, o Australijoje – net 942 kartus didesnė), bet ir skirtingos teisinės deliktinės atsakomybės rūšys (skirtingai nei likusiose valstybėse, JAV gali būti taikoma viena baudžiamosios teisės prievartos priemonių – laisvės atėmimas iki 5 m.). Kadangi teisės esmė yra teisių ir pareigų vienovė, todėl vienoje globalioje erdvėje padarius tokio paties pobūdžio teisės pažeidimą, teismams vykdant teisingumą, teisių ir pareigų pusiausvyra neturėtų būti atstatoma ribojant skirtingo lygio asmens subjektines teises;
- bausmės kai kuriose valstybėse yra per mažos, tai neprisideda prie *spam* platinimo prevencijos: Lietuvoje (2000 Lt) ir Rusijoje (1850 JAV dolerių) nustatyti sankcijų dydžiai neatitinka pažeidimo pavojingumo, lyginant su *spam* daroma žala.

3. Siekiant kovoti su *spam*, itin reikšmingas yra teisinio reguliavimo priemonių kūrimas ir jų taikymas, nes empirinis tyrimas parodė ir nepriklausomų statistikos agentūrų duomenys patvirtino, kad pastaruoju metu būtent iš tų valstybių (pvz., Rusijos, Argentinos, iš dalies,- Lietuvos), kurios neturi priėmusios specialiųjų teisės aktų, reglamentuojančių elektroninių komercinių pranešimų turinio siuntimą, yra vykdoma daugiausiai *spam* atakų, o to pasekmė – elektroninio pašto vartotojų teisių ir interesų pažeidimai, nepriklausomai nuo to, kurioje valstybėje jie gyvena ir kokie teisės aktai joje galioja.

4. Valstybėse galiojančių teisės aktų ir apskritai teisės spragomis nagrinėjamoje srityje aktyviai naudojasi *spam* siuntėjai ir problema nebus panaikinta tol, kol visos valstybės nepriims teisės aktų, reglamentuojančių nepageidaujamus ir pageidaujamus elektroninius komercinius pranešimus, jų siuntimą, atsakomybę bei elektroninio pašto savininko teisių gynimą

5. Atsižvelgiant į magistro baigiamojo darbo išvadas, siūloma *spam* problemą spęsti ne tik valstybiniu, bet ir tarptautiniu lygiu, kadangi internetas neapsiriboja atskirų valstybių teritorijomis ir yra globalaus pobūdžio.

§ Siekiant sumažinti *spam* problemą, turėtų būti aktyviau skatinamas teisės aktų harmonizavimas viso pasaulio mastu, tam reikia:
    - Ø priimti vieningą *spam* sąvoką;
    - Ø parinkti ir priimti vieningą („*opt-in*“, „*opt-out*“) metodą ar nustatyti gaires ir standartinius reikalavimus elektroninių (komercinių) pranešimų siuntimui, jų turiniui bei rekvizitams;

- Ø skatinti valstybių tarptautinį bendradarbiavimą, kurio tikslas būtų taikomų poveikio priemonių už su *spam* susijusius pažeidimus (nusikaltimus) standartizavimas.

§ Siekiant sumažinti *spam* plitimą, reikia nustatyti ir skirti pakankamo ir racionalaus dydžio baudas už *spam* reglamentuojančių teisės aktų nuostatų pažeidimus,

§ Atsižvelgiant į tai, kad visos valstybės turi prieigą prie vienos elektroninės erdvės ir minėtas problemas, kylančias dėl teisės aktų normų įvairovės, geriausia išeitis yra iškelti vieningo visame pasaulyje teisės akto – nepageidaujamų elektroninių pranešimų konvencijos – idėją.

LITERATŪROS SĄRAŠAS

Monografijos

1. A. Vaišvila. Teisės teorija. - Vilnius: Justitia, 2004. P. 446-447.
2. A. M. Gahtan, M.P.J. Kratz, J.F. Mann. Internet Law: A Practical Guide For Legal and Business Professionals. – Toronto: Carswell, 1998.P.177-187.
3. Diana Rowland, Elizabeth Macdonald. Information technology law: Third Edition, London Sydney Portland (Oregon): Cavendish Publishing, 2005. P. 385 – 386.
4. I. Jarukaitis, T.Lamanauskas, M. Civilka ir kt. Elektroninių ryšių teisė. – Vilnius: Eugrimas, 2005. P.352, 353, 356, 357.
5. L. Markauskas. Reklamos teisinis reglamentavimas: teorija ir praktika. –Vilnius: UAB „Mokesčių srautas“, 2008. P. 29, 159.
6. M. Kiškis, R. Petrauskas, I. Rotomskis ir kt. Teisės informatika ir informatikos teisė: vadovėlis. - Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006. P. 62, 125.
7. M. Civilka, T. Lamanauskas, G. Osinaitė ir kt. Informacinių technologijų teisė. - Vilnius: NVO Teisės institutas, 2004. P.93

Norminiai teisės aktai:

Lietuvoje ir ES:

1. Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37.
2. Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1998 O.J. (L 024) 1.
3. Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1.
4. Lietuvos Respublikos reklamos įstatymas // Valstybės žinios. 2000, Nr. 64-1937.
5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios. 1996, Nr. 63-1479.
6. Lietuvos Respublikos elektroninių ryšių įstatymas // Valstybės žinios. 2004, Nr. 69-2382.
7. Lietuvos Respublikos Baudžiamasis Kodeksas // Valstybės žinios. 1993, Nr. 12-296.

Australijoje

8. Can-Spam Act of 2003, No. 129 (Act Compilation - C2005C003882) // http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/DED153276FD7C6F9CA2570260013908A/$file/SpamAct03WD02.pdf; prisijungimo laikas: 2007-12-19.

9. Spam regulations 2004, Statutory rules 2004, No. 56 6/04/2004 // http://www.gov.mu/portal/sites/spamweb/download/Spam%20Regulations%202004.pdf; prisijungimo laikas: 2008-10-15.

10. Telecommunications Act 2053 B.S. (1996 A.D) (redakcija No. 47 ir No. 51, 2005) // http://www.nta.gov.np/telecom_act_2053.html; prisijungimo laikas: 2008-12-19.

11. Trade Practices Acto f 1974, No. 51. (redakcija No.119, 2005) // http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/0F2B9A313FE41C94CA25708B001BC4E7?OpenDocument; prisjungimo laikas 2008-02-19.

12. „Crimes Act 1914“ 4AA // http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s4aa.html; prisijungimo laikas: 2008-10-02.

Argentinoje:

13. Proteccion De Los datos Personales Nr. 25.326, 2000 // http://www.bcra.gov.ar/pdfs/marco/iHabeas%20Data.PDF; prisijungimo laikas: 2008-06-02

14. Argentine Constitution of 1994, section 43 // http://www.argentina.gov.ar/argentina/portal/documentos/constitucion_ingles.pdf; prisijungimo laikas: 2008-06-02.

15. Disposition Nº 1/2003. Data Protection infringements and penalties // http://www.protecciondedatos.com.ar/law12003.htm; prisijungimo laikas: 2008-10-15.

JAV:

16. Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act of 2003) 117 Stat. 2699 Public Law 108- 187- Dec. 16, 2003, 108th Congress// http://www.spamlaws.com/f/pdf/pl108-187.pdf; prisijungimo laikas 2007-12-19.

17. U.S.Code 18 Title – Crimes and Criminal procedure, 1037 straipsnis // http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I.html; prisijungimo laikas: 2008-02-19.

18. U.S.Code 15 Title – Commerce and Trade, 7704 straipsnis // http://www4.law.cornell. edu/uscode/uscode15/usc_sup_01_15_10_1.html; prisijungimo laikas: 2008-02-19.

Rusijoje:

19. The Civil Code of the Russian Federation. Art. 309 // http://www.russian-civil-code.com/; prisijungimo laikas: 2008-10-15.

20. Bill ‘On Legal Regulation of Rendering Internet Services‘.

21. Federal Law ‘On Communication‘ Nr. 126-FZ, 62 straipsnis // http://www.medialaw.ru/e_pages/laws/russian/communications.htm; prisijungimo laikas: 2008-10-15.

22. Konvencija dėl elektroninių nusikaltimų // Valstybės žinios, 2004-03-07, Nr. 36-1188.

23. 1948 m. Jungtinių Tautų Visuotinė Žmogaus teisių deklaracija // Valstybės žinios, 2006-06-17, Nr. 68-2497.

Šaltiniai Internete:

1. Apie spam faktais // http://www.esaugumas.lt/index.php?1812607726; prisijungimo laikas 2008-12-02.

2. The spam act and codes of practice // http://www.acma.gov.au/WEB/STANDARD/pc=PC_310321; prisijungimo laikas: 2008-01-20.

3. Federal Trade Commisision. Spam summit. July11-12, 2007 // http://www.ftc.gov/bcp/workshops/spamsummit/presentations/Law-Enf.pdf; prisijungimo laikas: 2008-01-30.

4. Malcolm Jeremy. Recent Developments in Australian Spam Law // http://www.isoc-au.org.au/Spam/SpamLaw.html; prisijungimo laikas: 2008-01-28.

5. US Department of Justice. Internacional Aspects of Computer Crime // http://www.cybercrime.gov/intl.html#Vb; prisijungimo laikas: 2008-01-30.

6. Operation spam zombies. London action plan // http://www.ftc.gov/bcp/conline/edcam s/spam/zombie/index.htm; prisijungimo laikas: 2008-01-28.

7. Personal data protection Act // http://dataprotection.blogspot.com/2003_11_01_dataprotection_archive.html; prisijungimo laikas: 2008-02-02.

8. ITU Activities on Countering Spam // http://www.itu.int/osg/spu/spam/; prisijungimo laikas: 2008-01-31.

9. Pablo Palazgi. Data Protection Law and Spam. First Spam case in Argentina // http://dataprotection.blogspot.com/2003_11_01_dataprotection_archive.html; prisijungimo laikas: 2008-02-02.

10. Judge in Argentina Orders Halt to Spamming in First E-Mail Junk Case // http://www.protecciondedatos.com.ar/bna.htm; prisijungimo laikas: 2008-02-02.

11. Legal status of a spam in Russia - 2005 AntiSpam Project' Annual Report // http://www.ifap.ru/eng/projects/as01.rtf; prisijungimo laikas: 2008-10-04.

12. Eugene Altovsky. Spam legislation in Russia“, 2006, IPOS UNESCO IFAP (Russia) // http://www.ifap.ru/eng/projects/as02.pdf; prisijungimo laikas: 2008-10-04.

13. Beveik 0,5 mln. kompiuterių pavirtę „zombiais“ // http://www.delfi.lt/archive/article.php?id=18432571; prisijungimo laikas: 2008-11-02.

14. The Federal Trade Commission. Opening Remarks of Deborah Platt Majoras „Developing A Plan for Action in the Fight Against Malicious Spam“, Spam Summit: The Next Generation of Threats and Solutions, July 11, 2007 // http://www.ftc.gov/bcp/workshops/spamsummit/presentations/Law-Enf.pdf; prisijungimo laikas 2008-01-30.

15. ICT regulation tolkit „Spam legislation“ // www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; prisijungimo laikas: 2008-07-23.

16. K. L. Hamilton, R. A. Fleck, Jr. Columbus state University. Can spam be legislated? // http://www.na-businesspress.com/hamiltonweb.pdf; prisijungimo laikas: 2008-11-12.

17. 29 straipsnio darbo grupės nuomonė 2/2006 apie privatumo klausimus susijusius su elektroninio pašto tikrinimo paslaugų teikimu // http://www.oecd.org/dataoecd/5/47/34935342.pdf; prisijungimo laikas: 2008-06-02.

18. E. Moustakas, prof. C..Ranganathan, Dr. Penny Duquenoy. Combating spam through legislation: a comparative anglysis of US and european approaches // http://www.ceas.cc/papers-2005/146.pdf; prisijungimo laikas: 2008-08-15.

19. Z. Medutis. Nepageidaujamų elektroninio pašto pranešimų studija // http://www.ada.lt/images/cms/File/Inspekcijos%20rekomendacijos/NEPP%20studija1.pdf; prisijungimo laikas: 2008-11-02.

20. Sophos Security threat report update 07/2008 // www.sophos.com/news/2008/07/dirtydozjul08.html; prisijungimo laikas: 2008-10-10.

21. Naumov V. Legal aspects of spam in Russia // http://www.russianlaw.net/english/ae06.htm; prisijungimo laikas: 2008-10-15.

22. Data protection law and spam. First spam case in Argentina // http://www.habeasdata.org/SpamEnglish; prisijungimo laikas: 2008-11-12.

23. http://lt.wikipedia.org/wiki/SMTP; prisijungimo laikas:2008-11-27.

24. Department of Justice FY 2007 Performance and accountability Report, P. 43. www.usdoj.gov/ag/annualreports/pr2007/msg-ag.pdf; prisijungimo laikas: 2008-11-12.

25. Apie spam faktais // http://www.esaugumas.lt/index.php?1812607726; prisijungimo laikas: 2008-11-02.

26. Metinė incidentų statistika. Ketvirtinė incidentų statistika // http://www.cert.lt/ statistika.html; prisijungimo laikas: 2008-11-02.

27. Regulation Toolkit. Spam Legislation // http://www.ictregulationtoolkit.org/en/Section.2081.html; prisijungimo laikas: 2008-07-02.

28. Idnetity fraud and identity theft // (http://www.cifas.org.uk/default.asp?edit_id=561-56); prisijungimo laikas: 2008-11-29.

29. Operation spam zombie // http://www.ftc.gov/bcp/conline/edcams/spam/zombie/translations/lithuanian.pdf; prisijungimo laikas: 2008-07-02.

30. Rekomendacijos „Ką daryti norint atsisakyti nepageidaujamų elektroninių žinučių?“ // http://www.ada.lt/images/cms/File/rekomendacijos_del_el_zinuciu.pdf; prisijungimo laikas: 2008-11-10.

31. Anoniminis naršymas per proxy serverius // http://proxy.uzeik.net/lt.php; prisijungimo laikas: 2008-12-02.

32. Vaitkus V. Spam problematika // http://www.rrt.lt/conferences/files/EC_2004_12_07_Vaitkus.pdf; prisijungimo laikas: 2008-01-16.

Teismų praktika:

1. EarthLink, Inc. V. Peter Moshou; Alice Cain; and John Does 1-25 (the timeshare spammers). (n.D. Ga. Filed Dec. 20, 2004).

2. Gustavo Daniel Tanús and Pablo Andrés Palazzi, c. Cosa, Carlos Alberto y Magraner, Ana Carolina s. Habeas Data, Federal Civil and Commercial Court No. 3, Secretariat No. 6.

3. LAT CBS teisėjų kolegijos 2001 m. gruodžio 12 d. nutartis c.b. Ž.Budros individuali įmonė „Sėkmės sistema“ v. UAB „D.B.S. Ltd.Pte“, Nr. 3K-3-1326/2001 m., kat. 31.4; 37.7; 49.1.

4. LAT BBS teisėjų kolegijos 2006 m. sausio 17 d. nutartis b.b. Nr. 2K-48/2006 m., kat. 1.2.30;2.4.2.1.

5. ROBERT H. BRAVER, Plaintiff, v. NEWPORT INTERNET MARKETING CORPORATION, and ROBERT ALAN SOLOWAY, Defendants, United States District Court #CIV-05-210-T.

6. Australian Communications and Media Authority v Clarity 1 Pty Ltd, [2006] FCA 1399).

SANTRAUKA

Šiame darbe nagrinėjama vis didėjanti elektroninės erdvės problema - nepageidaujamų elektroninių komercinių pranešimų – kitaip *spam* - platinimas, dėl kurio yra patiriami ne tik materialiniai nuostoliai, bet ir pažeidžiami asmens privatumo, orumo bei laisvo apsisprendimo principai, įtvirtinti valstybių konstitucijose, tarptautinėse konvencijose.

Pirmame skyriuje atskleidžiama *spam* samprata, jo savybės. Antrame skyriuje naudojantis lyginamuoju ir dokumentų analizės metodais, buvo analizuojami 5 pasaulio valstybių (Lietuvos, Australijos, Argentinos, JAV ir Rusijos) *spam* reglamentuojantys teisės aktai pagal pasirinktus kriterijus. Analizuojama, ar teisės aktuose *spam* įvardijamas ir suvokiamas kaip tas pats reiškinys, kiek plačiai yra reglamentuotas elektroninių komercinių pranešimų siuntimas bei turinys, ir kokių prievolių turi laikytis elektroninių komercinių pranešimų siuntėjai. Taip pat nagrinėjamos teisinės atsakomybės ribos, nustatytos už atitinkamų valstybių teisės aktuose įtvirtintų prievolių nesilaikymą ir elektroninio pašto vartotojų teisių pažeidimą, bei analizuojami jurisdikcijos elektroninėje erdvėje probleminiai kausimai.

Siekiant išsiaiškinti, ar užsakomi ir gaunami elektroniniai komerciniai pranešimai praktikoje atitinka minėtų valstybių teisės aktuose numatytus reikalavimus, buvo atliktas empirinis tyrimas, kurio programa, tyrimo eiga, rezultatai bei išvados pateikiami ketvirtame skyriuje.

Be to, darbe nagrinėjamas savireguliacijos bei tarpininkų vaidmuo, pateikiami teismų praktikos pavyzdžiai, naujausios, grėsmę keliančios *spam* platinimo formos, aktualiausia statistinė informacija.

Magistro baigiamojo darbo išvadose pateikiami galimi *spam* problemos sprendimo būdai, teisinės situacijos gerinimo galimybės.

Pagrindinės sąvokos: nepageidaujamas elektroninis komercinis pranešimas (*spam*), *anti-spam* teisės aktai, sutikimo (angl. *opt-in)* ir atsisakymo (angl. *opt-out)* metodai, išankstinis sutikimas, atsisakymo mechanizmas.

SUMMARY

In this Master‘s thesis an increasing problem of electronic universe – the spread of unsolicited Electronics commercial emails, otherwise called spam - is analyzed. Due to this not only material losses are incurred, but also person‘s privacy, dignity and free will principles that are enshrined in various constitutions, International conventions are breached.

Conception and qualities of spam are revealed in the first chapter. In the second one, legal acts regulating spam in 5 countries (Lithuania, Australia, Argentina, the USA and Russia) were analyzed using comparative and document analysis methods and in accordance to chosen criteria. It was examined whether spam is called and perceived in the same way in various legal acts, as well as how broadly the contents and sending of spam is regulated, what are the established duties for senders of electronic commercial email. Besides, boundaries of legal liabilities, that are set in case of non compliance to legal requirements and violations of rights of the users of email, are researched. Problematic issues of jurisdiction in electronic universe are discussed.

An empirical survey was carried out in order to investigate if in practice subscribed electronic commercial emails are in compliance with the legal acts of the above mentioned countries. The program, course of actions, results and findings are disclosed in the fourth chapter.

In addition, the role of self-regulation and the responsibilities of intermediaries are analyzed, as well as cases of court practice, newest and threatening forms of distribution of spam, relevant statistical data are presented.

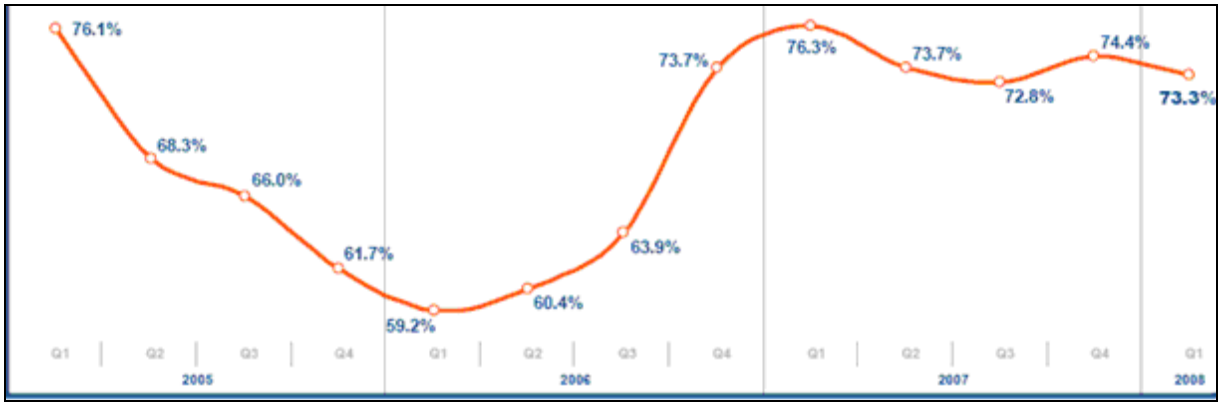
To conclude, possible means of solving spam related problems and prospects of possible improvements are laid.

Key words: unsolicited commercial electronic message (spam), anti-spam laws, opt-in and opt-out approaches, prior consent, unsubscribe mechanism.

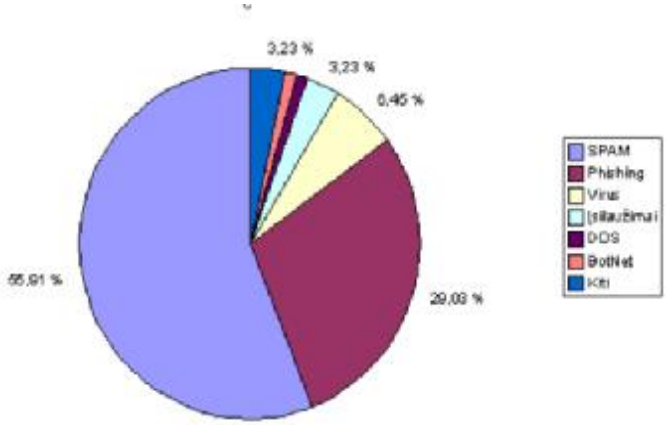
PRIEDAI

Priedas Nr.1. **2005-2008 m. *spam* pasiskirstymas (www.esaugumas.lt)**

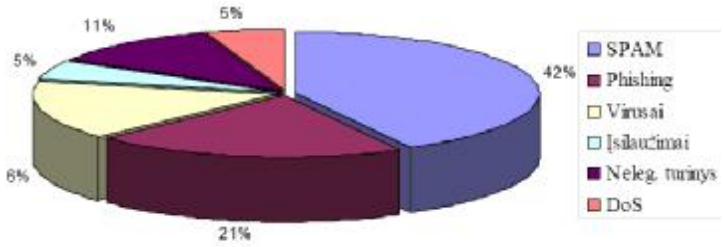
MessageLabs statistika: *spam* 2008 metais sudaro apie 73,3 proc. visų elektroninio pašto laiškų:



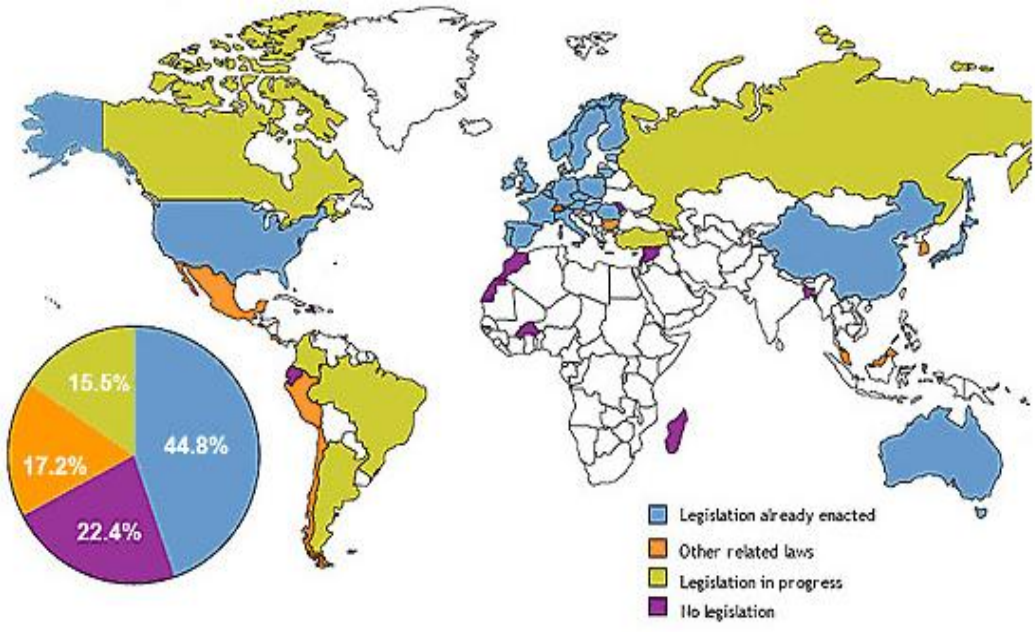
2006 m. incidentų statistika CERT tyrimų grupės duomenimis (www.cert.lt)



2007 m. incidentų statistika CERT tyrimų grupės duomenimis (www.cert.lt)



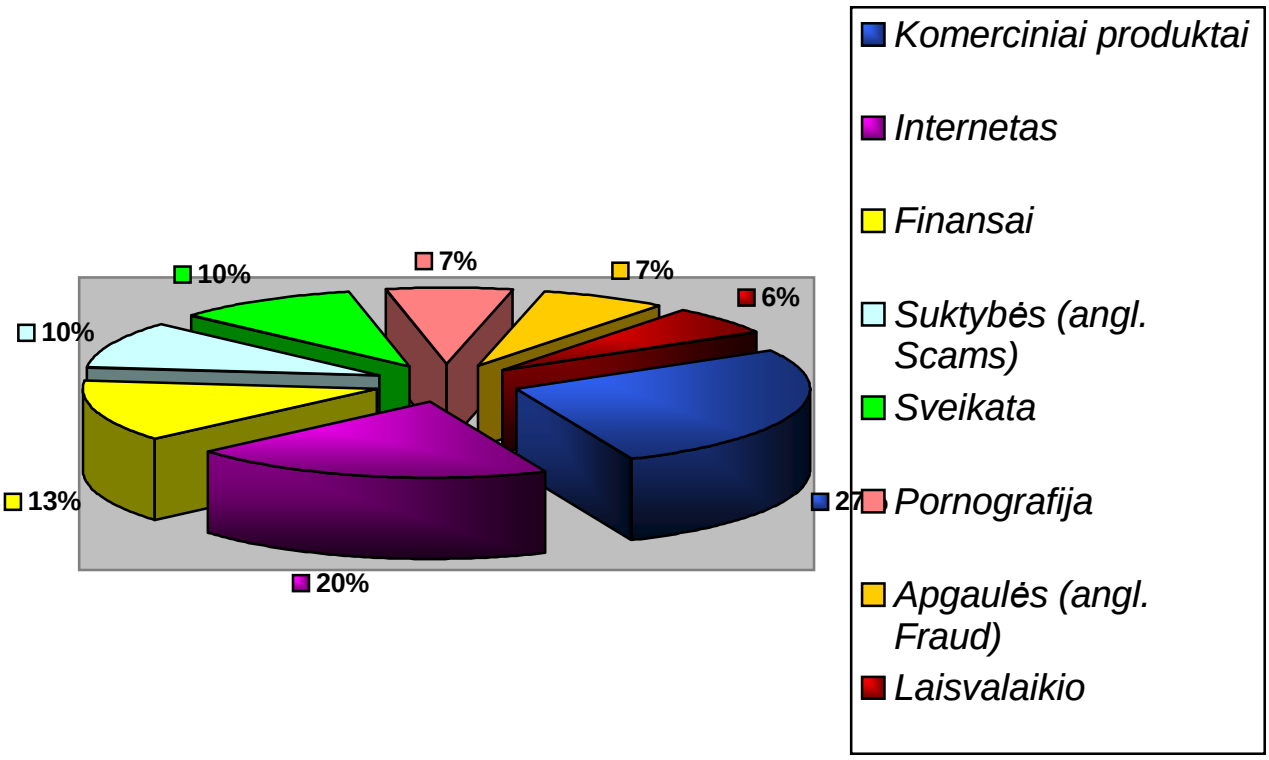
Priedas Nr. 2. **Atskirų valstybių *spam* teisės aktų leidyba**[50].



- (mėlyna) spalva pažymėtos valstybės yra priėmusios *spam* reglamentuojančius teisės aktus.
- (morkine) spalva pažymėtos valstybės pasitelkia alternatyvius teisės aktus *spam* reglamentuoti.
- (žalia) spalva pažymėtos valstybės rengia *spam* reglamentuojančius teisės aktų projektus.
- (violetine) spalva pažymėtos valstybės apskritai neturi jokių *spam* reglamentuojančių teisės aktų.

[50] ICT Regulation Toolkit. Spam Legislation // http://www.ictregulationtoolkit.org/en/Section.2081.html; prisijungimo laikas: 2008-07-02.

Priedas Nr. 3. **Spam kategorijos**



Informacija pasinaudota iš http://www.esaugumas.lt

Priedas Nr. 4. **Socialiniais internetiniais puslapiais platinamos neatpažįstamos reklamos pavyzdys**

Facebook spam

Informacija paimta iš Sophos Security threat report update 07/2008 // www.sophos.com/news/2008/07/dirtydozjul08.html; prisijungimo laikas: 2008-10-10.

Priedas Nr. 5. **Teisės aktų lyginamosios analizės santrauka**.

	Taikomas metodas	Priimtuose teisės aktuose spam įvardijamas kaip...	Ar numatytas atgalinio adreso įtraukimas?	Ar numatytas privalomas fizinio adreso įtraukimas?	Ar numatyta pateikti informaciją apie siuntėją?	Kokie numatyti atsisakymo funkcijai įgyvendinti papildomi reikalavimai?	Ar numatytas išankstinis reklamos identifikavimas antraštėje (angl.*subject line*)?	Ar numatyti tam tikri reikalavimai tik suaugusiems skirtiems (riboto turinio) pranešimams?	Atsakomybė
Lietuva	Opt-in	„neužsakytas komercinis pranešimas“ arba „elektroninis pranešimas, skirtas tiesioginės rinkodaros tikslams“	Taip (arba pagal LR elektroninių ryšių įstatymą yra numatyta alternatyva nurodyti tik tapatybę)	Ne	Numatyta alternatyva: pateikti arba atgalinį adresą, arba informaciją apie siuntėjo tapatybę	Nemokamai ir paprastomis priemonėmis;	Ne	Ne	Administracinė, civilinė
Australija	Opt-in	unsolicited commercial electronic messages	Taip	Taip	Taip	1.Trumpas pareiškimas; 2.Pareiškimas lengvai ir aiškiai pastebimas; 3.Adresas turi galioti 30d; 4. el. adresas yra teisėtai įgytas. 5.”unsubscribe” mechanizmas.	Ne	Ne	Administracinė, civilinė
Argentina	Opt-out	-	Ne	Ne	Ne	Nenumatyta	Ne	Ne	Administracinė,

									civilinė
JAV	Opt-out	unsolicited commercial electronic mail message	Taip	Taip	Taip	1.aiškiai pastebimas „unsubscribe" mechanizmas ir jo aprašymas; 2. 30 dienų terminas; 3. „saugus prieglobstis" siuntėjams;	Taip	Taip	Civilinė, baudžiamoji
Rusija	Opt-in	informacijos platinimas, pagal kurį siuntėjas tiksliai nežino, kas yra šios informacijos gavėjas.	Ne	Ne	Ne	Nenumatyta	Taip	Ne	Administracinė, civilinė

Priedas Nr. 6: lentelė Nr. 1.**JAV sukurto elektroninio pašto vardene.pavardene@mail.com empirinio tyrimo duomenys**

JAV įmonės	„Unsubscribe“ mechanizmas	Atgalinio adreso įtraukimas	Fizinio adreso įtraukimas	Informacija apie siuntėją	Teisinga antraštė	Iš viso gauta pranešimų	Atsisakymo sudėtingumas
Kelionių agentūros Nr. 1 pranešimai	+	+	+	+	+	11	N
Kelionių agentūros Nr. 2 pranešimai	+	+	+	+	+	11	N
Naujienų agentūros Nr.1 pranešimai	+	+	+	+	+	17	N
Naujienų agentūros Nr 2. pranešimai	+	+	+	+	+	11	N
Suaugusiems skirto internetinio puslapio Nr. 1 pranešimai	-	+	-	-	-/+	4	S
Suaugusiems skirto internetinio puslapio Nr. 2 pranešimai	+	+	-	-	-/+	1	N
IT elektroninė parduotuvė Nr.1	+	+	+(pašto dėžutė)	+	+	6	N
IT elektroninė parduotuvė Nr. 2	+	+	+(pašto dėžutė)	+	+	4	N

65 laiškai +1 (nekilnojamojo turto agentūros) gautas papildomai, 66 laiškai

Priedas Nr. 6: lentelė Nr. 2. **Australijoje sukurto elektroninio pašto vardene.pavardene@inthemix.com.au empirinio tyrimo duomenys**

Australijos įmonės	„Unsubscribe“ mechanizmas	Atgalinio adreso įtraukimas	Fizinio adreso įtraukimas	Informacija apie siuntėją	Teisinga antraštė (nereikalaujama)	Iš viso gauta pranešimų	Atsisakymo sudėtingumas
Kelionių agentūros Nr. 1 pranešimai	+	+	+	+	+	7	N
Kelionių agentūros Nr. 2 pranešimai	+	+	+	+	+	5	N
Naujienų agentūros Nr.1 pranešimai	+	+	+	+	+	25	LS+ 3 nepageidauti po 1 atsisakymo
Naujienų agentūros Nr 2. pranešimai	+	+	-	+	+	17	N
Suaugusiems skirto internetinio puslapio Nr. 1 pranešimai)	+	+	+	+	+	6	N
Suaugusiems skirto internetinio puslapio Nr. 2 pranešimai	+	+	-	-	+	4	N
IT elektroninė parduotuvė Nr.1	+	+	+	+	+	6	N
IT elektroninė parduotuvė Nr. 2	+	+	+	+	+	1	N

71 laiskas + naujienų agentūros Nr. 1 reikėjo atsisakyti per du kartus. Po pirmo atsisakymo gauti 3 laiškai, iš viso 74.

Priedas Nr. 6: lentelė Nr. 3. **Lietuvoje sukurto elektroninio pašto vardene.pavardene@inbox.lt empirinio tyrimo duomenys**

Lietuvos įmonės	„Unsubscribe“ mechanizmas	Atgalinio adreso įtraukimas	Fizinio adreso įtraukimas	Informacija apie siuntėją	Teisinga antraštė	Iš viso gauta pranešimų	Atsisakymo sudėtingumas
Kelionių agentūros Nr. 1 pranešimai	+	+	+	+	+	25	N
Kelionių agentūros Nr. 2 pranešimai	+	+	+	+	+	8	N
Naujienų agentūros Nr.1 pranešimai	-	+	-	-	+	15	LS+12 spam
Naujienų agentūros Nr 2. pranešimai	+	+	+	+	+	20+2 prenumerata (tapačios prekes)	N
Suaugusiems skirto internetinio puslapio Nr. 1 pranešimai	-	+	-	-	-/+	2	S
Suaugusiems skirto internetinio puslapio Nr. 2 pranešimai	+	+	-	-	-/+	1	N
IT elektroninė parduotuvė Nr.	+	+	+ (pašto dėžutė)	+	+	4	N
IT elektroninė parduotuvė Nr. 1	+	+	+ (pašto dėžutė)	+	+	3	N

gauti 80 laiškų + 12 (Naujienų agentūra Nr. 1) + 3 (neužsakyti pranešimai), iš viso 95.

Priedas Nr. 6: lentelė Nr. 4. **Argentinoje sukurto elektroninio pašto vardene.pavardene@cuidad.ar empirinio tyrimo duomenys**

Argentinos įmonės	„Unsubscribe“ mechanizmas	Atgalinio adreso įtraukimas	Fizinio adreso įtraukimas (nereikalaujama)	Informacija apie siuntėją (nereikalaujama)	Teisinga antraštė (nereika-laujama)	Iš viso gauta pranešimų	Atsisakymo sudėtingumas
Kelionių agentūros Nr. 1 pranešimai	+	+	-	+	+	30	LS+(9+4) spam
Kelionių agentūros Nr. 2 pranešimai)	+	+	+	+	+	1	N
Naujienų agentūros Nr.1 pranešimai	+	+	-	-	+	1	N
Naujienų agentūros Nr. 2. pranešimai	+	+	-	-	+	43	N
Suaugusiems skirto internetinio puslapio Nr. 1 pranešimai	+	+	-	-	+	1	N
Suaugusiems skirto internetinio puslapio Nr. 2 pranešimai	+	+	-	-	+	1	N
IT elektroninė parduotuvė Nr.1	+	+	-	+	+	1	N
IT elektroninė parduotuvė Nr. 2	+	+	+	-	+	3	N

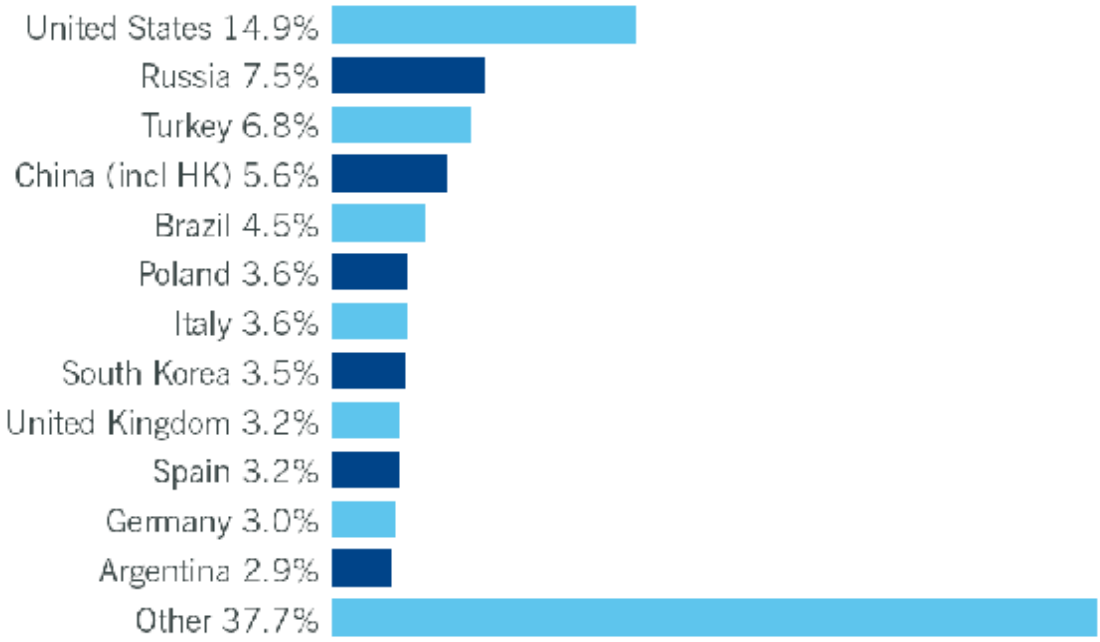
Gauta iš viso 81 laiškai +13 spam (po atsisakymo), iš viso 94

Priedas Nr. 6: Lentelė Nr. 5**. Rusijoje sukurto elektroninio pašto vardene.pavardene@rambler.ru empirinio tyrimo duomenys**

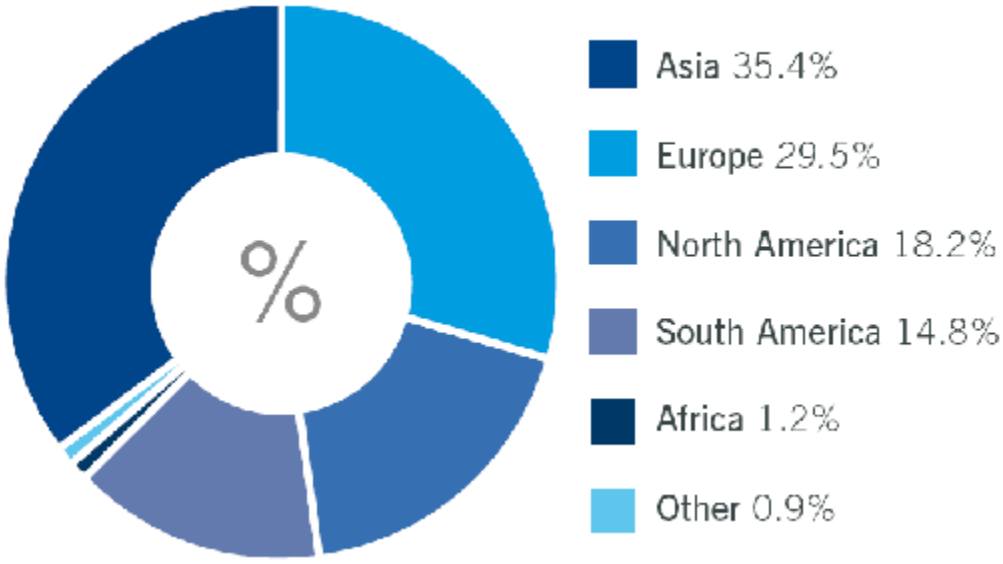
Rusijos įmonės	„Unsubscribe“ mechanizmas	Atgalinio adreso įtraukimas	Fizinio adreso įtraukimas (nereikalaujama)	Informacijos apie siuntėją pateikimas (nereikalaujama)	Teisingos antraštės reikalavimas	Iš viso gauta pranešimų	Atsisakymo sudėtingumas
Kelionių agentūros Nr. 1 pranešimai	-	+	-	+	+	5	S
Kelionių agentūros Nr. 2 pranešimai	+	+	-	-	+	2	N
Naujienų agentūros Nr.1 pranešimai	+	+	-	-	+	32	LS+6 spam
Naujienų agentūros Nr 2. pranešimai	-	+	-	-	+	4	LS+ 4 spam
Suaugusiems skirto internetinio puslapio Nr. 1 pranešimai	+	+	-	-	+	1	N
Suaugusiems skirto internetinio puslapio Nr. 2 pranešimai	-	+	-	-	+	1	S
IT elektroninė parduotuvė Nr.1	+	+	+	+	+	1	N
IT elektroninė parduotuvė Nr. 2	-	+	+	-	+	3	S

Iš viso gauti 49 laiskas + 10 spam, + 1 (neužsakytas) iš viso 60

Priedas Nr. 7. ***Spam* siuntimo statistika pagal atskiras valstybes**.



***Spam* siuntimo statistika pagal atskirus kontinentus**:



Informacija pasinaudota iš: Sophos Security threat report update 07/2008 // www.sophos.com/news/2008/07/dirtydozjul08.html; prisijungimo laikas: 2008-10-10.